

THE ROLE OF THE WHITE HOUSE
CHIEF TECHNOLOGY OFFICER IN
THE HEALTHCARE.GOV WEBSITE DEBACLE

HEARING
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

NOVEMBER 19, 2014

Serial No. 113-96

Printed for the use of the Committee on Science, Space, and Technology



THE ROLE OF THE WHITE HOUSE
CHIEF TECHNOLOGY OFFICER IN
THE HEALTHCARE.GOV WEBSITE DEBACLE

HEARING
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

NOVEMBER 19, 2014

Serial No. 113-96

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

92-329PDF

WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRBACHER, California	EDDIE BERNICE JOHNSON, Texas
RALPH M. HALL, Texas	ZOE LOFGREN, California
F. JAMES SENSENBRENNER, JR., Wisconsin	DANIEL LIPINSKI, Illinois
FRANK D. LUCAS, Oklahoma	DONNA F. EDWARDS, Maryland
RANDY NEUGEBAUER, Texas	FREDERICA S. WILSON, Florida
MICHAEL T. McCAUL, Texas	SUZANNE BONAMICI, Oregon
PAUL C. BROUN, Georgia	ERIC SWALWELL, California
STEVEN M. PALAZZO, Mississippi	DAN MAFFEI, New York
MO BROOKS, Alabama	ALAN GRAYSON, Florida
RANDY HULTGREN, Illinois	JOSEPH KENNEDY III, Massachusetts
LARRY BUCSHON, Indiana	SCOTT PETERS, California
STEVE STOCKMAN, Texas	DEREK KILMER, Washington
BILL POSEY, Florida	AMI BERA, California
CYNTHIA LUMMIS, Wyoming	ELIZABETH ESTY, Connecticut
DAVID SCHWEIKERT, Arizona	MARC VEASEY, Texas
THOMAS MASSIE, Kentucky	JULIA BROWNLEY, California
KEVIN CRAMER, North Dakota	ROBIN KELLY, Illinois
JIM BRIDENSTINE, Oklahoma	KATHERINE CLARK, Massachusetts
RANDY WEBER, Texas	
CHRIS COLLINS, New York	
BILL JOHNSON, Ohio	

SUBCOMMITTEE ON OVERSIGHT

HON. PAUL C. BROUN, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin	DAN MAFFEI, New York
BILL POSEY, Florida	ERIC SWALWELL, California
KEVIN CRAMER, North Dakota	SCOTT PETERS, California
BILL JOHNSON, Ohio	EDDIE BERNICE JOHNSON, Texas
LAMAR S. SMITH, Texas	

CONTENTS

November 19, 2014

Witness List	Page 2
Hearing Charter	3

Opening Statements

Statement by Representative Paul C. Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	8
Written Statement	9
Statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	10
Written Statement	12
Statement by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	13
Written Statement	14

Witnesses:

Mr. Todd Park, former Chief Technology Officer of the United States, Office of Science and Technology Policy (OSTP)	
Oral Statement	15
Submitted Biography	18
Discussion	25

Appendix I: Answers to Post-Hearing Questions

Mr. Todd Park, former Chief Technology Officer of the United States, Office of Science and Technology Policy (OSTP)	50
---	----

Appendix II: Additional Material for the Record

Prepared statement by Representative Eric Swalwell, Committee on Science, Space, and Technology, U.S. House of Representatives	80
Supporting documents submitted by Representative Paul C. Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	82
Hearing documents submitted by the Majority staff, Committee on Science, Space, and Technology, U.S. House of Representatives	155
Letter submitted by Representative Scott Peters, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	193
Minority staff report submitted by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	195
Majority staff report submitted by Representative Paul C. Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	413

**THE ROLE OF THE WHITE HOUSE
CHIEF TECHNOLOGY OFFICER IN
THE HEALTHCARE.GOV WEBSITE DEBACLE**

WEDNESDAY, NOVEMBER 19, 2014

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:10 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Paul Broun [Chairman of the Subcommittee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
BANKING MEMBER

**Congress of the United States
House of Representatives**

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

***The Role of the White House Chief Technology Officer in the
HealthCare.gov Website Debacle***

Wednesday, November 19, 2014
10:00 a.m. to 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Mr. Todd Park, former Chief Technology Officer of the United States, Office of
Science and Technology Policy (OSTP)

U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight

HEARING CHARTER

*The Role of the White House Chief Technology Officer
in the HealthCare.gov Website Debacle*

Wednesday, November 19, 2014
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

On Wednesday, November 19, 2014, the Subcommittee on Oversight will hold a hearing titled, *The Role of the White House Chief Technology Officer in the HealthCare.gov Website Debacle*.

On September 17, 2014, the Subcommittee on Oversight approved a resolution to authorize the issuance of a subpoena *ad testificandum* to Mr. Todd Park, former Chief Technology Officer (CTO) of the United States, Office of Science and Technology Policy (OSTP). The subpoena compels Mr. Park's appearance before the Subcommittee to explain his role in the development and rollout of the HealthCare.gov website that Health and Human Services (HHS) Secretary Kathleen Sebelius called a "debacle"¹ with a recently estimated cost of over \$2 billion.² Despite Mr. Park denying knowledge of security and testing concerns with HealthCare.gov prior to the rollout of the website, the Committee has reviewed many emails where Mr. Park demonstrates an in-depth knowledge of these issues prior to October 1, 2013. This hearing will cover what Mr. Park knew and what he reported to other senior White House officials.

In late August, the White House announced that Mr. Park would step down as CTO to take a new role in the Administration as technical advisor to the White House, working from Silicon Valley.

Witness

- **Mr. Todd Park**, former Chief Technology Officer of the United States, Office of Science and Technology Policy

¹ Bill Chappell, "Sebelius Calls For Review of HHS Practices That Led To Debacle," NPR, December 11, 2013, available at: <http://www.npr.org/blogs/thetwo-way/2013/12/11/250207327/sebelius-calls-for-review-of-hhs-practices-that-led-to-debacle>.

² Alex Wayne, "Obamacare Website Costs Exceed \$2 Billion, Study Finds," Bloomberg, September 24, 2014, available at: <http://www.bloomberg.com/news/2014-09-24/obamacare-website-costs-exceed-2-billion-study-finds.html>.

Background

As U.S. CTO, Mr. Park declined five invitations to testify before the Committee about his knowledge and involvement with the development of HealthCare.gov, including its cybersecurity standards and protocols. Over the course of several letters, OSTP has claimed:

- It “has not been substantially involved in the privacy and security standards that are in place for healthcare.gov.”³
- Neither “Mr. Park nor any other OSTP staff member is in a position to testify on the data security standards of the website. Indeed, when asked about the security features of the HealthCare.gov website during a hearing...before another committee, Mr. Park explained that he has not been working on these issues.”⁴
- Mr. Park and “OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace’s (FFM) security measures....Mr. Park is not a cybersecurity expert; he did not develop or approve the security measures in place to protect the website, and he does not manage those responsible for keeping the site safe.”⁵

Further, while testifying under oath when subpoenaed by the Oversight and Government Reform Committee last November, Mr. Park said that he did not “actually have a really detailed knowledge base” of the website before it was launched and was “not deeply familiar with the development and testing regimen that happened prior to October 1.”⁶

However, documents received by the Science Committee over the summer and this past month from the Committee’s subpoena of Mr. Park’s records raise serious questions of Mr. Park’s denial that he was not knowledgeable or familiar with the development, testing, and security concerns relative to the HealthCare.gov website.

HealthCare.gov

On October 1, 2013, under the provisions of the Patient Protection and Affordable Care Act (ACA), the Administration launched HealthCare.gov, a federally-operated health insurance exchange website to help uninsured people find health care coverage.

The data passing through the HealthCare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies as well as state agencies and government contractors. When launched last year, users attempting to gain information on potential healthcare coverage through the website were required to input

³ November 8, 2013, Letter from OSTP to SST Committee.

⁴ November 14, 2013 Letter from OSTP to SST Committee.

⁵ July 3, 2014, Letter from OSTP to SST Committee.

⁶ “Obamacare Implementation – The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, November 13, 2013, available at: <http://oversight.house.gov/hearing/obamacare-implementation-rollout-healthcare-gov>.

personal contact information, birth dates and social security numbers for all family members, in addition to household salary, and other personal data.

Federal agencies have an obligation to ensure that these private records have sufficient protection from misuse and security breaches under the Federal Information Security Management Act (FISMA). However, according to documents from the Department of Health and Human Services (HHS), the security of the healthcare website had not been fully tested when it was launched last year,⁷ and cybersecurity experts at a November 2013 hearing before the Science Committee expressed concern about flaws in the website that put the personal data of Americans using the website at risk of identity theft from cybercriminals/hackers.⁸

The Committee oversees the agencies responsible for setting cyber privacy and security policies and standards for the rest of the federal government - the National Institute for Standards and Technology (NIST) and the White House Office of Science and Technology Policy.

On October 31, 2013, the Committee sent the first letter to Mr. Todd Park, then-U.S. CTO,⁹ requesting that he testify at a hearing on November 19, 2013, to address the Committee's concerns about the lack of privacy standards for personal information passing through the HealthCare.gov website and the threat posed to Americans if hackers on the Internet gained access to such information. The Committee's specific interest in questioning Mr. Park was based on several factors:

- Prior to his position as U.S. CTO, Mr. Park was the CTO at HHS, where he "led the successful execution of an array of breakthrough initiatives, including the creation of HealthCare.gov."¹⁰
- As the U.S. CTO, Mr. Park worked at OSTP and was considered part of OSTP leadership. While there he focused on "how technology policy and innovation can advance the future of our nation."¹¹ According to his biography, previously available on OSTP's website, Mr. Park is "a highly accomplished health IT entrepreneur"¹² who together with Mr. Jeff Zients, "assembled and led the tech surge that overhauled HealthCare.gov, ultimately enabling millions of Americans to sign up for quality, affordable health insurance."¹³
- In written testimony before the Committee two years ago, Dr. John Holdren, OSTP Director, explained that:

⁷ Robert Pear and Eric Lipton, "Health Website Official Tells of White House Briefings," The New York Times, November 13, 2013, available at: http://www.nytimes.com/2013/11/14/us/officials-say-they-dont-know-cost-of-health-website-fixes.html?_r=0.

⁸ Matthew J. Belvedere, "No Security Ever Built Into Obamacare Site: Hacker," CNBC.com, November 25, 2013, available at: <http://www.cnbc.com/id/101225308>.

⁹ Mr. Park resigned his position as U.S. CTO on August 29, 2014, per an e-mail from OSTP to the Committee.

¹⁰ White House Blog, "Todd Park Named New U.S. Chief Technology Officer," March 9, 2012, available at: <http://www.whitehouse.gov/blog/2012/03/09/todd-park-named-new-us-chief-technology-officer>.

¹¹ OSTP website, Todd Park bio, previously available at:

<http://www.whitehouse.gov/administration/eop/ostp/about/leadershipstaff/park>.

¹² Ibid.

¹³ Ibid.

“OSTP also supports me in my role as Assistant to the President for Science and Technology and the U.S. Chief Technology Officer, who sits in OSTP, in our functions advising the President on S&T dimensions of the policy challenges before the Nation, including strengthening the economy and creating jobs, improving healthcare and education, enhancing the quality of the environment, and advancing national and homeland security.”¹⁴

The Science Committee’s interest in hearing from Mr. Park intensified with the acquisition of documents from the Oversight and Government Reform Committee that identified Mr. Park as a White House co-chair of the Affordable Care Act Information Technology Exchanges Steering Committee.¹⁵ According to these documents, the stated mission of this HealthCare.gov Steering Committee is to support the timely and efficient resolution of barriers to assure the implementation of “consumer-centric” health insurance exchanges. The Steering Committee’s Charter explicitly directs its participants “to promote resolution to key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government and with the state exchanges,” and to “direct the formulation of work groups to identify barriers, develop or identify promising practices to support efficiencies, and develop option papers for the Committee’s consideration.” The ACA Exchanges Steering Committee oversees both security and privacy interagency working groups.

Previous Hearings

When the site was launched on October 1, 2013, it was plagued with operational problems. In light of the myriad problems facing the website, on November 19, 2013, the Committee held a hearing to explore the threat posed by identity theft to Americans if hackers acquired such information through the HealthCare.gov website.¹⁶ The hearing also examined issues related to the website’s security controls and potential vulnerabilities by inviting cybersecurity experts to discuss what specific security standards and technical measures should be in place to protect Americans’ privacy and personal information on HealthCare.gov.

The Committee revisited these issues in a subsequent hearing on January 16, 2014,¹⁷ which provided Members with an updated assessment of HealthCare.gov to determine the likelihood of personal information being accessed or compromised from an attack on the website. The hearing also examined the potential consequences of identity theft to Americans if hackers with malicious intent gained personal information through the website. At the conclusion of the hearing, Chairman

¹⁴ SST hearing, “Examining the Priorities and Effectiveness of the Nation’s Science Policies,” June 20, 2012, available at: <http://science.house.gov/hearing/full-committee-hearing-examining-priorities-and-effectiveness-nation%E2%80%99s-science-policies>.

¹⁵ SST Majority Staff Report, “Did the White House Knowingly Put Americans’ Sensitive Information at Risk? Committee Seeks to Clarify Contradictions Surrounding Senior White House Official’s Role in Developing HealthCare.gov,” October 2014, available at: <http://science.edgeboss.net/sst2014/documents/October%202014%20Todd%20Park%20Majority%20Staff%20Report.pdf>.

¹⁶ SST hearing, “Is My Data on Healthcare.gov Secure?” November 19, 2013, available at: <http://science.house.gov/hearing/full-committee-hearing-my-data-healthcaregov-secure>.

¹⁷ SST hearing, “Healthcare.gov: Consequences of Stolen Identity,” January 16, 2014, available at: <http://science.house.gov/hearing/full-committee-hearing-healthcaregov-consequences-stolen-identity>.

Smith called on the President to formally certify the safety requirements, security standards and privacy conditions of HealthCare.gov.

Questions Remain

One year later, concerns about the HealthCare.gov website's security still remain with the second Open Enrollment period for HealthCare.gov. Despite the improved functionality since the flawed October 1st launch, it is unclear how much work has been done to address the privacy and security aspects of that functionality, which were concerns raised in the Committee's prior hearings.

- According to news reports over the past few months, the Centers for Medicare and Medicaid Services "denied a request by *The Associated Press* under the Freedom of Information Act for documents about the kinds of security software and computer systems behind the federally funded HealthCare.gov."¹⁸
- News stories in September also reported that a "hacker broke into part of the HealthCare.gov insurance enrollment website in July and uploaded malicious software."¹⁹
- A recent U.S. Government Accountability Office review of the website made the following observation: "Healthcare.gov had weaknesses when it was first deployed, including incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternate processing site to avoid major service disruptions."²⁰ This report also finds: "[W]eaknesses remain both in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls."²¹
- And in a recent news conference, the President reportedly said, "We're really making sure the website works super well before the next open enrollment period. We're double-and triple-checking it."²² However, the same news article reports that while HealthCare.gov performed better than last year, consumers in Virginia for example, "were having a hard time logging into their accounts retrieving old passwords and proving they were who they said they were – a process known as identity proofing, which also vexed many people last fall."²³

¹⁸ Jack Gillum, "US Won't Reveal Records on Health Website Security," Associated Press, August 21, 2014, available at: <http://www.federalnewsradio.com/458/3684543/US-wont-reveal-records-on-health-website-security>.

¹⁹ Danny Yadron, "Hacker Breached HealthCare.gov Insurance Site," *The Wall Street Journal*, September 4, 2014, available at: <http://online.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043>.

²⁰ "HealthCare.gov – Actions Needed to Address Weaknesses in Information Security and Privacy Controls," GAO, September 16, 2014, available at: <http://www.gao.gov/products/GAO-14-730>.

²¹ *Ibid.*

²² Robert Pear and Abby Goodnough, "Some New Frustrations as Health Exchange Opens," *New York Times*, November 15, 2014, available at: <http://www.nytimes.com/2014/11/16/us/health-insurance-marketplace-opens.html?rref=us&module=ArrowsNav&contentCollection=U.S.&action=keypress®ion=FixedRight&pgtype=article>.

²³ *Ibid.*

Chairman BROUN. This hearing of the Subcommittee on Oversight will come to order. Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Good morning, and welcome to today's hearing. In front of you are packets containing the written testimony, biography, and truth-in-testimony disclosure for today's witness. I now recognize myself for five minutes for an opening statement.

I want to thank my colleagues for being here today, and I want to especially thank our witness for his presence. We have been waiting a very long time to be able to question you, sir. I am sorry that we had to come to the point of issuing you a subpoena to get that to happen, but I am glad that you are here today, sir.

In fact, the Committee has invited you several times before on five different occasions. We wrote directly to you, Mr. Park, as well as to the Director of the Office of Science and Technology Policy. None of those invitations elicited the "yes" response that we got as a result of issuing you a subpoena.

In the course of our correspondence, several claims were made by OSTP as to why you were not the individual to answer the Committee's questions, such as: that you and OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace's security measures; that you did not develop or approve the security measures in place to protect the website; that you do not manage those responsible for keeping the site safe; and that you are not a cybersecurity expert, which is an interesting description of you to say the least. You are the co-founder of Athenahealth, which you co-developed into one of the most innovative health IT companies in the industry and become very wealthy, in fact, doing that. As a government employee, you helped launch the President's Smarter IT Delivery Agenda, which created the new U.S. Digital Service, and you created the beta version of HealthCare.gov. How do these activities not require cybersecurity expertise?

Further, on November 13, 2013, in testimony, sworn testimony, before the Committee on Oversight and Government Reform, you said that you did not, to quote you, "actually have a really detailed knowledge base" of the website before it was launched, and that you were, again quoting you, "not deeply familiar with the development and testing regimen that happened prior to October 1."

However, the Committee has in its possession documents that appear to contradict much of what you have said in your prior Congressional appearance, again under oath, as well as what OSTP has explained to this Committee.

But these documents were not easy to come by, despite requesting them in a letter last December, and despite preparing to ask about them in a briefing OSTP arranged on your behalf in September—a briefing that was canceled the evening before it was scheduled to take place when your colleagues were informed it would be transcribed.

Mr. Park, I find your and the White House's lack of transparency intolerable and an obstruction to this Committee's efforts to conduct oversight. It took a subpoena to get you here, sir. It took another subpoena to compel your documents from the White House, but even with that, we have yet to receive all of your documents

in compliance with our subpoena issued on September 19, exactly 2 months ago.

As a gesture of good faith, Committee staff have engaged in multiple in-camera reviews with White House lawyers, yet there are still documents being withheld from the Committee without a claim of a legally recognized privilege. That begs the question: What are you hiding, Mr. Park?

I have some theories about the answer to that question. Perhaps it is that you knew there were serious problems with HealthCare.gov prior to the launch but you did not convey them up the chain in your briefings with the President. Or, perhaps you did, and they were ignored because of this Administration's relentless pursuit to launch HealthCare.gov on October 1, 2013, no matter the consequences.

Now here we are, a year later and fresh into the beginning of the second open enrollment, with questions that still remain about this \$2 billion debacle you are credited with fixing—a debacle that, I might add, got hacked this summer and that, according to a recent Government Accountability Office report, still has weaknesses, as they say “both in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls.”

We look forward to this opportunity to ask you some of our questions, Mr. Park.

I also now ask unanimous consent to submit documents for the record, which will be referenced in some of our questions. Without objection, so ordered.

[The information appears in Appendix II]

Chairman BROWN. Before I yield to the Ranking Member, Eddie Bernice Johnson, my friend from Texas, and because of some conflict with the Democrats, we will come back to Mr. Swalwell's statement later on, I might add that this is likely my last time chairing this Subcommittee on Oversight for a hearing, and I would like to thank my friends on both sides of the aisle, especially Chairman Smith, for a productive two years of hard work on this Subcommittee. Our staff, both Democrat and Republican, worked very hard. We worked together in as bipartisan manner as possible. We might not have agreed on all the issues. Some issues we did, some we didn't. But it has been a very productive two years, I think, and I have been very privileged to Chair this Subcommittee. I wish you all well next year.

[The prepared statement of Mr. Broun follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT
CHAIRMAN PAUL BROWN

Good morning. I want to thank my colleagues for being here today and I want to especially thank our witness for his presence—we have been waiting a very long time to question you, sir.

In fact, the Committee has invited you to testify before us on five different occasions. We wrote directly to you, Mr. Park, as well as to the Director of the Office of Science and Technology Policy. None of those invitations elicited the “yes” response we got as a result of issuing you a subpoena.

In the course of our correspondence, several claims were made by OSTP as to why you were not the individual to answer the Committee's questions, such as:

- That you and OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace's security measures;
- That you did not develop or approve the security measures in place to protect the website;
- That you do not manage those responsible for keeping the site safe; and
- That you are not a cybersecurity expert—which is an interesting description of you to say the least. You are the co-founder of Athenahealth, which you co-developed into one of the most innovative health IT companies in the industry. As a government employee, you helped launch the President's Smarter IT Delivery Agenda, which created the new U.S. Digital Service, and you created the beta version of HealthCare.gov—how do these activities not require cybersecurity expertise?

Further, on November 13, 2013, in testimony before the Committee on Oversight and Government Reform, you said that you did not “actually have a really detailed knowledge base” of the website before it was launched, and that you were “not deeply familiar with the development and testing regimen that happened prior to October 1.”¹

However, the Committee has in its possession documents that appear to contradict much of what you have said in your prior Congressional appearance, as well as what OSTP has explained to this Committee.

But these documents were not easy to come by, despite requesting them in a letter last December, and despite preparing to ask about them in a briefing OSTP arranged on your behalf in September—a briefing that was cancelled the evening before it was scheduled to take place when your colleagues were informed it would be transcribed.

Mr. Park, I find your and the White House's lack of transparency intolerable and an obstruction to this Committee's efforts to conduct oversight. It took a subpoena to get you here. It took another subpoena to compel your documents from the White House, but even with that, we have yet to receive all of your documents in compliance with our subpoena issued on September 19th, exactly two months ago. As a gesture of good faith, Committee staff have engaged in multiple in camera reviews with White House lawyers, yet there are still documents being withheld from the Committee without a claim of a legally recognized privilege. That begs the question—what are you hiding, Mr. Park?

I have some theories about the answer to that question. Perhaps it is that you knew there were serious problems with HealthCare.gov prior to the launch but you did not convey them up the chain in your briefings with the President. Or, perhaps you did, and they were ignored because of this Administration's relentless pursuit to launch HealthCare.gov on October 1, 2013, no matter what the consequences.

Now here we are, a year later and fresh into the beginning of the second Open Enrollment, with questions that still remain about this \$2 billion dollar debacle you are credited with fixing—a debacle that, I might add, got hacked this summer and that, according to a recent Government Accountability Office report, still has weaknesses “both in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls.”

We look forward to this opportunity to ask you some of our questions.

Before I yield to Mr. Swalwell for his opening statement, let me just add that this is likely my last time chairing an Oversight Subcommittee hearing, and I would like to thank my friends on both sides of the aisle—especially Chairman Smith—for a productive two years of hard work on this Subcommittee. I wish you all well next year, and I now recognize Mr. Swalwell.

Chairman BROUN. I now recognize our Ranking Member, Ms. Eddie Bernice Johnson, for her statement. You are recognized for five minutes.

Ms. JOHNSON. Thank you, Mr. Chairman, and let me express my appreciation for your service, since this might very well be your last chairing of this Committee, and wish you well in the future.

¹“Obamacare Implementation—The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, November 13, 2013, available at: <http://oversight.house.gov/wp-content/uploads/2014/06/11-13-13-TRANSCRIPT-Obamacare-Implementation-The-Rollout-of-HealthCare.gov—pdf>.

We have maintained a great relationship, although I must say that probably 99.9 percent of the time we disagree.

But I want to welcome Mr. Park, the former Chief Technology Officer of the United States, to this Committee hearing, and I appreciate, Mr. Park, your willingness to appear before us. I want to apologize to you for all the political theater that is unfolding around your appearance. Please keep in mind that this hearing is largely an excuse for the majority to again express their dislike for the Affordable Care Act and the online Marketplace that has led millions of Americans to find medical coverage. I know that they do not like Obamacare. The Majority has voted at least some 53 times during this Congress to repeal or dismantle the ACA.

Nevertheless, I want to ask all Members here today to please remember that Mr. Park is not personally responsible for the ACA, nor is he responsible for the problems on October 1, 2013.

Mr. Park, it is clear that you were not responsible for how the website performed last October 1st. In doling out responsibility for its performance on day one, I think it was fair to assign you zero percentage of the responsibility, which reflects the degree of your actual involvement in developing the website.

Of course, your job at the White House put you in a position to have more insight than most into how the Centers for Medicare and Medicaid Services were doing in developing the program, but the management of the program was up to CMS. And the people doing the actual development work were contractors who legally answered to CMS. As I am sure you would agree, insight into what is going on does not equate to being intimately involved or directly responsible for the website. And of course your real job as CTO during that period had you leading multiple interagency initiatives designed to push technology into the American economy and across society. For example, you were working to make U.S. government data more easily accessible by the public, which can spur innovation, profits and jobs, as has been amply demonstrated by the way that publicly available National Weather Service data has spawned a multibillion-dollar weather forecasting industry.

Mr. Park, I think it is fair to say that fundamentally you were working to make services of the government more readily available to citizens during your tenure as CTO. You were working to help reduce information costs in various areas of the economy, notably your green button initiative to let consumers get a better idea about energy consumption and sourcing. You were facilitating dialogues across communities to bring experts on particular social issues face-to-face with experts from the IT world. Laudably, you were a part of an initiative aimed at stopping human trafficking and another initiative designed to find ways to harness IT more effectively in disaster response.

I know that as I cite these examples, I am just scratching the surface of the scope of your day job as CTO of the United States. Regrettably, the Committee has made no effort to understand this broad portfolio of your accomplishments there, and has shown little appreciation for your patriotic desire to serve, even though it meant leaving the lucrative world of Silicon Valley IT startups and venture capital. From the bottom of my heart, I want to thank you

for all you did and tried to do, including joining the team tasked with fixing the HealthCare.gov site after October 1st.

I hope your experience with this Committee won't diminish your sense of pride in your accomplishments or dampen your enthusiasm for public service. We need people like you to be willing to come serve this country.

Thank you, and I yield back.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF FULL COMMITTEE
RANKING MEMBER EDDIE BERNICE JOHNSON

Mr. Chairman, I want to welcome Mr. Park, the former Chief Technology Officer of the United States, to this Committee hearing. I appreciate your willingness to appear before us, Mr. Park, and I want to apologize to you for all the political theater that is unfolding around your appearance.

Please keep in mind that this hearing is largely an excuse for the Majority to again express their dislike for the Affordable Care Act and the online-Marketplace that has let millions of Americans find medical coverage. I know that they do not like Obamacare—the Majority have voted in the House some 53 times during this Congress to repeal or dismantle the ACA. Nevertheless, I want to ask all Members here today to please remember that Mr. Park is not personally responsible for the ACA, nor is he responsible for the problems on October 1, 2013.

Mr. Park, it is clear that you were not responsible for how the website performed last October 1. In doling out responsibility for its performance on day one I think it's fair to assign you 0 % of the responsibility, which reflects the degree of your actual involvement in developing the website.

Of course, your job at the White House put you in a position to have more insight than most into how the Centers for Medicare and Medicaid Services were doing in developing the program, but the management of the program was up to CMS. And the people doing the actual development work were contractors who legally answered to CMS. As I'm sure you would agree, insight into what is going on does not equate to being intimately involved or directly responsible for the website.

And of course your real job as CTO during that period had you leading multiple interagency initiatives designed to push technology out into the American economy and across society. For example, you were working to make U.S. government data more easily accessible by the public, which can spur innovation, profits, and jobs, as has been amply demonstrated by the way that publicly available National Weather Service data has spawned a multi-billion dollar weather forecasting industry.

Mr. Park, I think it is fair to say that fundamentally you were working to make services of the government more readily available to citizens during your tenure as CTO. You were working to help reduce information costs in various areas of the economy, notably your "green button" initiative to let consumers get a better idea about energy consumption and sourcing. You were facilitating dialogues across communities to bring experts on particular social issues face-to-face with experts from the IT world. Laudably, you were a part of an initiative aimed at stopping human trafficking and another initiative designed to find ways to harness IT more effectively in disaster response.

I know that as I cite these examples, I am just scratching the surface of the scope of your day job as CTO of the United States. Regrettably, the Committee has made no effort to understand this broad portfolio or your accomplishments there, and has shown little appreciation for your patriotic desire to serve, even though it meant leaving the lucrative world of Silicon Valley IT start-ups and venture capital.

From the bottom of my heart, I want to thank you for all you did and tried to do, including joining the team tasked with fixing the healthcare.gov site after October 1. I hope your experience with this Committee won't diminish your sense of pride in your accomplishments or dampen your enthusiasm for public service. We need people like you to be willing to come serve the country.

Chairman BROWN. Thank you, Ms. Johnson. I disagree with you about a couple of issues. One is that we have recognized Mr. Park's accomplishments and responsibilities outside of being involved in HealthCare.gov. In fact, he himself has said he has not been deeply involved, though there are emails that we have and that you have

that show otherwise. So it is not zero involvement, and it seems to be the mantra of this Administration that people are zero involved and have no responsibility for issues, but thank you, Ms. Johnson.

I now recognize the full Committee Chairman, Mr. Lamar Smith, for five minutes.

Chairman SMITH. Thank you, Mr. Chairman.

Americans have seen firsthand the misrepresentations that surround Obamacare. First, there was the President's broken promise that "If you like your health care plan, you can keep it." Then, in a video that surfaced last week, MIT professor Jonathan Gruber, a principal architect of Obamacare, admitted how the Administration sold this to the American people, saying "Lack of transparency is a huge political advantage. Basically, call it the stupidity of the American voter or whatever, but basically that was really, really critical to getting the thing [Obamacare] to pass."

Finally, after a year of requests by this Committee, the Administration has agreed to have someone who worked in the White House testify about the lack of security of the HealthCare.gov website. Mr. Todd Park was the White House Chief Technology Officer for the Office of Science and Technology Policy from March 2012 to August 2014.

Joining the Obama Administration in the Department of Health and Human Services, Mr. Park was one of the principal architects for the HealthCare.gov website. Former Health and Human Services Secretary Kathleen Sebelius later called this website "a debacle" with a recent estimated cost of \$2 billion.

Today we will review the White House's repeated misinformation about the HealthCare.gov website. Mr. Park's own emails show an in-depth, detailed knowledge about cybersecurity issues with the website. He was the primary spokesperson for the White House about the website and the website's security. Mr. Park directed several contractors to review the security of the website.

On October 10th, soon after the website went operational, Mr. Park read an online article by David Kennedy, a white hat hacker who has testified twice before this Committee. Mr. Kennedy's article was titled "Is the Affordable Care Website Secure? Probably Not." Mr. Park commented in an email how he was advised that "these guys are on the level." We are asking Mr. Park to explain his role in developing the \$2 billion website and what the Administration knew about the security risks of the website.

As of today, the White House still has failed to provide this Committee with all the documents that are subject to the subpoena. The ones we do have paint a far different picture than that of the Office of Science and Technology Policy.

As I mentioned, the Committee has not received all of the emails and other documents that were subject to the subpoena so another hearing may well be necessary.

Finally, I want to take a moment to thank the Chairman of the Oversight Subcommittee, Dr. Paul Broun, for his tireless efforts on this subject as well as so many other subjects that have come before this Subcommittee. We appreciate his public service and his dedication over the years to his constituents, to Congress, and to our country. So Chairman Broun, thank you again for all you have

done. We appreciate all your great work, and I look forward to today's hearing.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF FULL COMMITTEE CHAIRMAN LAMAR S. SMITH

Americans have seen first-hand the misrepresentations that surround Obamacare. First, there was the President's broken promise that "If you like your health care plan, you can keep it."

Then, in a video that surfaced last week, MIT professor Jonathan Gruber, a principal architect of Obamacare, admitted how the Administration sold this to the American people, saying:

"Lack of transparency is a huge political advantage. Basically, call it the stupidity of the American voter or whatever, but basically that was really, really critical to getting the thing [Obamacare] to pass."

Finally, after a year of requests by this Committee, the Administration has agreed to have someone who worked in the White House testify about the lack of security of the HealthCare.gov website. Mr. Todd Park was the White House Chief Technology Officer for the Office of Science and Technology Policy (OSTP) from March 2012 to August 2014.

Joining the Obama Administration in the Department of Health and Human Services, Mr. Park was one of the principal architects for the HealthCare.gov website. Former Health and Human Services (HHS) Secretary Kathleen Sebelius later called this website "a debacle" with a recent estimated cost of \$2 billion.

Today we will review the White House's repeated misinformation about the HealthCare.gov website.

Mr. Park's own emails show an in-depth, detailed knowledge about cybersecurity issues with the website. He was the primary spokesperson for the White House about the website and the website's security.

Mr. Park directed several contractors to review the security of the website. On October 10th—soon after the website went operational—Mr. Park read an online article by David Kennedy, a white hat hacker who has testified twice before this Committee.

Mr. Kennedy's article was entitled "Is the Affordable Care Website Secure? Probably Not." Mr. Park commented in an email how he was advised that "these guys are on the level."

We're asking Mr. Park to explain his role in developing the \$2 billion website and what the Administration knew about the security risks of the website.

As of today, the White House still has failed to provide this Committee with all the documents that are subject to the subpoena. The ones we do have paint a far different picture than that of the Office of Science and Technology Policy.

As I mentioned, the Committee has not received all of the emails and other documents that were subject to the subpoena. So another hearing may well be necessary.

Finally, I want to take a moment to thank the chairman of the Oversight Subcommittee, Dr. Paul Broun, for his tireless efforts on this subject and many others before the Oversight Subcommittee. We appreciate his public service and dedication over his many years on the Science Committee.

I look forward to today's hearing.

Chairman BROWN. Thank you, Mr. Smith. As I announced earlier, Mr. Swalwell will be joining us in a bit, and he will give his opening statement at that time and then ask his questions in due order. If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

At this time, I would like to introduce today's witness, Mr. Todd Park, the former Chief Technology Officer of the United States and Assistant to the President. Prior to this role, Mr. Park served as Chief Technology Officer for the U.S. Department of Health and Human Services, and before entering Federal service, Mr. Park co-founded Athenahealth and co-led its development into one of the most impressive health IT companies in the industry.

As our witness should know, spoken testimony is limited to five minutes after which the members of the Committee will have five minutes each to ask questions. And Mr. Park, it is the practice of this Subcommittee on Oversight to receive testimony under oath. If you now would please stand and raise your right hand? Do you solemnly swear and affirm to tell the whole truth and nothing but the truth, so help you God?

Mr. PARK. I do.

Chairman BROWN. Thank you. You may be seated. Let the record reflect that the witness answered in the affirmative and has taken the oath.

I now recognize Mr. Park for five minutes to present your testimony, sir.

**TESTIMONY OF TODD PARK,
FORMER CHIEF TECHNOLOGY OFFICER
OF THE UNITED STATES,
OFFICE OF SCIENCE AND TECHNOLOGY POLICY**

Mr. PARK. Thank you, sir.

Chairman Broun, thank you for your service. Chairman Smith, Ranking Member Swalwell, Ranking Member Johnson and Members of the Committee, good morning. I am looking forward to the opportunity to offer testimony to you today.

To begin, I would like to provide some context for my time as U.S. Chief Technology Officer that will be helpful in addressing questions you have asked me to answer.

I am a private-sector health IT entrepreneur by background and have been blessed with significant success in that arena. Only in America can the son of two brave immigrants from Korea have the kind of business-building experiences that I have been blessed to have. I love this country very much, and it has been the greatest honor of my life to serve it.

In March 2012, after 2-1/2 years working at the U.S. Department of Health and Human Services, I joined the White House Office of Science and Technology Policy as U.S. CTO. In this role, my primary job was to serve as a Technology Policy and Innovation Advisor across a broad portfolio of issues, working on open data policy and initiatives, wireless spectrum policy, how to advance a free and open Internet, how to harness the power of technological innovation to fight human trafficking and improve disaster response and recovery, and more. My role as U.S. CTO was not to oversee the internal Federal IT budget and operations. However, given my background at HHS and as a health IT entrepreneur, I was asked to provide assistance to CMS, which was the agency in charge of managing the development of the new HealthCare.gov including the Federally Facilitated Marketplace for Health Insurance. I provided assistance to CMS in a few different capacities.

For example, I served as one of three co-chairs of an interagency steering committee organized by the Office of Management and Budget and which focused on providing a neutral venue in which agencies like CMS, IRS, SSA and others could work through inter-agency items, primarily in support of the Data Services Hub, which ended up going live quite successfully. I assisted with a Red Team exercise in early 2013 that helped identify actions to improve

project execution as well as some associated follow-on work that summer. From time to time I helped connect people to each other, served as a spokesperson of sorts, and provided help on particular questions.

However, to properly calibrate your expectations of my knowledge of CMS's initial development of the new HealthCare.gov and the Federally Facilitated Marketplace, I was not a project manager who was managing and executing the day-in and day-out operational work of building the new HealthCare.gov and the Federally Facilitated Marketplace. This was the responsibility of CMS. I didn't have the kind of comprehensive, deep, detailed knowledge of the effort that a hands-on project manager would have, and which I have had about other projects in my private-sector work.

I assisted CMS with its work as an advisor while executing my overall duties as White House Technology Policy Innovation Advisor working on a broad range of policy issues as I described earlier.

As the new HealthCare.gov and the Federally Facilitated Marketplace rolled out in the fall of 2013, as the extent of operational issues with the site became clear, it became an all-hands-on-deck moment, and I along with others dropped everything else I was doing and increased my involvement in HealthCare.gov dramatically, shifting full time into the HealthCare.gov turnaround effort and working as part of a tech surge, which radically improved the performance of the site. I worked as part of a terrific team working around the clock, even sleeping on office floors. My particular focus was on helping to reduce the amount of time the site was down, improve the site's speed, improve its ability to handle high user volume, and improve user-facing functionality. Our team effort drove massive improvement in the site, ultimately enabling millions of Americans to sign up for health insurance through the site, many of whom had previously been uninsured.

At the end of the day on April 15, 2014, the last day of extended special enrollment, I went back to my U.S. CTO day job of being Technology Policy and Innovation Advisor, and my involvement in HealthCare.gov accordingly scaled back dramatically.

As another contextual note, I understand that the Committee's primary interest has been the security of HealthCare.gov. I do not have the expertise in cybersecurity that the professors of cybersecurity and other experts who previously testified before this Committee have. Responsibility for the cybersecurity of HealthCare.gov rests with CMS. My involvement with the security of HealthCare.gov has been rather tangential. The interagency steering committee I co-chaired had a privacy and security subgroup but the subgroup was staffed and led by Agency personnel who occasionally asked the overall committee co-chairs to help facilitate interagency dialog and cooperation but who generally drove to the ultimate answers themselves. There were a small number of other occasions when I was asked to serve as a spokesperson of sorts—summarizing general cybersecurity content supplied by CMS and HHS—to function as a liaison or facilitator connecting people to each other, or to provide my general thoughts for whatever they were worth. But, again, I am not a cybersecurity expert.

As a final contextual note, at the end of August of this year, in order to stay married, I stepped down as U.S. CTO and returned

home to Silicon Valley, fulfilling my wife's longstanding desire to do so. I continue to serve our country as a consultant to the White House based in Silicon Valley, focused primarily on attracting more and more of the best tech talent in the Nation to serve the American people, which is important to our vital work as a government to radically improve how the government delivers digital services and unleashes the power of technology in general.

Thank you for the opportunity to provide some context for my testimony today, and I look forward to answering your questions as best I can.

[The prepared statement of Mr. Park follows:]

Chairman Broun, Chairman Smith, Ranking Member Maffei, Ranking Member Johnson, and Members of the Committee, good morning. I'm looking forward to the opportunity to offer testimony to you today.

To begin, I would like to provide some context for my time as United States Chief Technology Officer (CTO) that will be helpful in addressing questions you've asked me to answer.

I am a private-sector health IT entrepreneur by background, and have been blessed with significant success in that arena. Only in America can the son of two brave immigrants from Korea have the kind of business-building experiences that I have been blessed to have.

In August 2009, I was asked to come serve our country, the country I love so very much, as the U.S. Department of Health and Human Service's (HHS) Chief Technology Officer (CTO) and "entrepreneur-in-residence." My role at HHS was to serve as a technology policy and innovation advisor. My principal focus there was on open data policy – making health care-related data and knowledge more open and accessible to help fuel innovation, entrepreneurship, and health care

improvement. As a special project, after the passage of the Affordable Care Act in March 2010, I was also asked to lead an early effort to develop a website in 90 days that provided basic information about the Affordable Care Act and health coverage options. This website was the first edition of HealthCare.gov, and was a purely informational site; it did not contain a transactional marketplace in which people applied for health insurance. This early website went live very successfully on July 1, 2010. I should note that, subsequently, this website was essentially completely replaced in 2013 by the Centers for Medicare and Medicaid Services (CMS) with a new HealthCare.gov that incorporated the Federally Facilitated Health Insurance Marketplace.

In March 2012, I joined the White House Office of Science and Technology Policy as U.S. CTO. In this role, my primary job was to serve as a technology policy and innovation advisor across a broad portfolio of issues, working on open data policy and initiatives, wireless spectrum policy, how to advance a free and open internet, how to harness the power of technological innovation to fight human trafficking and improve disaster response and recovery, and more. My role as U.S. CTO was not to oversee the internal Federal IT budget and operations. However, given my background at HHS and as a health IT entrepreneur,

I was asked to provide assistance to CMS, which was the agency in charge of managing the development of the new HealthCare.gov, including the Federally Facilitated Marketplace for health insurance.

I provided assistance to CMS in a few different capacities. For example, I served as one of three co-chairs of an interagency steering committee, organized by the Office of Management and Budget (OMB) and which focused on providing a neutral venue in which agencies like CMS, IRS, SSA and others could work through interagency items -- primarily in support of the data services hub, which ended up going live quite successfully. I assisted with a "red team" exercise in early 2013 that helped identify actions to improve project execution, as well as some associated follow-on work that summer. From time to time, I helped connect people to each other, served as a spokesperson of sorts, and provided help on particular questions.

However, to properly calibrate your expectations of my knowledge of CMS's initial development of the new HealthCare.gov and Federally Facilitated Marketplace: I was not a project manager who was managing and executing the day-in and day-out operational work of building the new HealthCare.gov and the Federally Facilitated

Marketplace. This was the responsibility of CMS. I didn't have the kind of comprehensive, deep, detailed knowledge of the effort that a hands-on project manager would have, and which I have had about other projects in my private sector work. I assisted CMS with its work as an advisor, while executing my overall duties as White House technology policy and information advisor, working on a broad range of policy issues, as I described earlier.

As the new HealthCare.gov and the Federally Facilitated Marketplace rolled out in the fall of 2013, as the extent of the operational issues with the site became clear, it became an all-hands on deck moment, and I, along with others, dropped everything else I was doing and increased my involvement in HealthCare.gov dramatically, shifting full-time into the HealthCare.gov turnaround effort, and working as part of the "tech surge" that radically improved the performance of the site.

I worked as part of a terrific team, working around the clock, even sleeping on office floors. My particular focus was on helping to reduce the amount of time the site was down, improve the site's speed, improve its ability to handle high user volume, and improve user-facing functionality. Our team effort drove massive improvement in the site, ultimately enabling millions of Americans to successfully sign up for

health insurance through the site -- many of whom had previously been uninsured.

At the end of the day on April 15, 2014, the last day of extended special enrollment, I went back to my U.S. CTO day job of being technology policy and innovation advisor, and my involvement in HealthCare.gov accordingly scaled back dramatically.

As another contextual note, I understand that the committee's primary interest has been the security of HealthCare.gov. I do not have the expertise in cybersecurity that the professors of cybersecurity and other experts who previously testified before this Committee have. Responsibility for the cybersecurity of HealthCare.gov rests with CMS. As you know, each federal agency has responsibility for the security of its sites, as each agency is closest to the ground and the operations of its programs. My involvement with the security of HealthCare.gov has been rather tangential. The interagency steering committee I co-chaired had a privacy and security subgroup, but this subgroup was staffed and led by agency personnel, who occasionally asked the overall committee co-chairs to help facilitate interagency dialogue and cooperation, but who generally drove to the ultimate answers

themselves. There were a small number of other occasions when I was asked to serve as a spokesperson of sorts (summarizing general cybersecurity content supplied by CMS and HHS), to function as a liaison or facilitator connecting people to each other, or to provide my general thoughts for whatever they were worth. But, again, I am not a cybersecurity expert.

As a final contextual note, at the end of August of this year, in order to stay married, I stepped down as U.S. CTO and returned home to Silicon Valley, fulfilling my wife's longstanding desire to do so. I continue to serve our country as a consultant to the White House based in Silicon Valley, focused primarily on attracting more and more of the best tech talent in the Nation to serve the American people – which is important to our vital work as a government to radically improve how the government delivers digital services and unleashes the power of technology in general.

Thank you for the opportunity to provide some context for my testimony today, and I look forward to answering your questions as best I can.

Todd Park

Todd Park is a consultant to the White House based in Silicon Valley, a role in which he has served since the end of August, 2014. Park's focus is on recruiting more top tech talent like [Mikey Dickerson](#) into government and identifying innovative ways to improve the quality of government digital services, two central goals of the President's [Smarter IT Delivery agenda](#). He is also helping to ensure that the Administration has an on-the-ground sense of how technology is evolving and can craft policy and initiatives accordingly.

Prior to this role, Todd Park served as the U.S. Chief Technology Officer (CTO) in the White House Office of Science and Technology Policy from 2012-2014. In this role, he served as an Assistant to the President. As U.S. CTO, Park focused on how technology policy and innovation can advance the future of our nation.

Park joined the Administration in August 2009 as Chief Technology Officer of the U.S. Department of Health and Human Services (HHS). In this role, he served as a change agent and "entrepreneur-in-residence," helping HHS harness the power of data, technology, and innovation to improve the health of the nation. Prior to joining HHS, Mr. Park co-founded Athenahealth and co-led its development into one of the most innovative health IT companies in the industry. He also co-founded Castlight Health, a web-based health care shopping service for consumers.

Park also served in a volunteer capacity as a Senior Fellow at the Center for American Progress, where he focused on health IT and health reform policy, and as senior health care advisor to Ashoka, a leading global incubator of social entrepreneurs, where he helped start Healthpoint Services, a venture to bring affordable telehealth, drugs, diagnostics, and clean water to rural India. Mr. Park graduated magna cum laude and Phi Beta Kappa from Harvard College with an A.B. in economics.

Chairman BROUN. Thank you, Mr. Park, for your testimony. Reminding members that Committee rules limit questioning to five minutes, the Chair at this point will open the round of questions. The Chairman recognizes himself for five minutes.

Mr. Park, let us clarify something. You claim in your opening statement today that you did not have, to quote you, “comprehensive, deep, detailed knowledge” of development, testing and cybersecurity of HealthCare.gov website and that you “assisted CMS with its work as an advisor.” Yet if you refer to tab 8 in your binder there, you can read along from the highlighted sections of one of your subpoenaed emails dated June 26, 2013, sent to Marilyn Tavener, Michele Snyder and Henry Chao about “a deep-dive session with Henry Chao.” Specifically, you wrote, “Marilyn, I’m also going to visit with Henry and team for one of our evening deep-dive sessions to get up to speed on the latest status of IT and testing. There’s no substitute for an evening deep dive. So I’ll bring healthy food and snacks to Baltimore and camp out with Henry and team for a few hours.”

Mr. Park, please explain to me how you define “deep, detailed knowledge” and then contrast that with a deep-dive experience with Mr. Chao and that lasts for several hours.

Mr. PARK. Sir, I would be delighted to. So in my private-sector experience, when you have really deep, detailed, comprehensive knowledge of a project, that comes from being the project manager. That comes from being the person who is in charge of running things, you know what is going on, you know each axis of what is going on on an ongoing basis, and that is the role I served in my private-sector life on a variety of projects but that was not the role I was serving on the Federally Facilitated Marketplace. That was CMS’s responsibility.

What is happening here is that on a few occasions, I spent time with the folks who were actually running the project and asked a series of questions and got information but that level of knowledge pales in comparison to the really deep, detailed, comprehensive knowledge that you would have as the project manager running the thing on an ongoing basis.

Chairman BROUN. So you had some supervisory function there.

Mr. Park, do you agree with Health Secretary Kathleen Sebelius’ assessment that the rollout of the website was “a debacle”?

Mr. PARK. The rollout was unacceptable, sir.

Chairman BROUN. Mr. Park, you acknowledge in your opening statement that you were one of three White House co-chairmen of the Affordable Care Act Information Technology Exchanges Steering Committee, and that at least initially met on a monthly basis. What was your role in these meetings? Would you say that you were the leader of this White House trio?

Mr. PARK. I would say that I was one of the three co-chairs. It was actually principally led and organized by the Office of Management and Budget, and the role of the committee was to focus on providing a neutral venue where agencies could come together and work on really interagency issues, primarily in support of the Data Services Hub.

Chairman BROUN. Well, on April 11, 2013, in an email sent at 2:31 p.m.—that is in tab 1—

Mr. PARK. Thank you, sir.

Chairman BROUN. —of your binder, with the subject “Coordination on ACA,” one of the co-chairs, Mr. Steven VanRoekel, then U.S. Chief Information Officer, expressed his concerns about your closeness to the Centers for Medicare and Medicaid Services by writing this: “CMS has not been inclusive and is not leading a coordinated effort that will lead to success. I am also worried that you are getting a too-CMS-centric picture. I would love nothing more than this not to be the case, to be assured ACA implementation is on a path we want to be on, and that existing efforts will deliver what we want.”

Your response to him sent the same day at 4:58 p.m. states, “Hey, brother. Thanks so much for the note and the chat! Many apologies for not staying in tighter sync with you on this. Will make sure we stay in close sync going forward.”

To be clear, this is the same CMS that the Office of Science and Technology Policy has told the Committee in various letters is in a “far better position to discuss the standards that are in place for the website.”

You did not deny this closeness to Mr. VanRoekel, and indeed, your closeness to individuals such as Henry Chao, Chief Information Officer at CMS, and Michele Snyder, then Chief Operating Officer at CMS and the number two official, is evident in the many emails we have seen of your conversations with them.

If you were not the leader, then why was Mr. VanRoekel looking toward you for guidance? And if you were so close to CMS that it concerned your co-chair, then surely you are in just fine a position to answer our questions about the website and should have done so a year ago?

Mr. PARK. So thank you for the opportunity to discuss this particular email. As I recall, I think this was precipitated by the fact that I had assisted, as I said in my opening testimony, the Red Team exercise CMS had engaged in to basically assess risks and identify mitigative actions to mitigate those risks in early 2013. Steve was actually not involved with that, and he was expressing concern about the fact that he wasn’t synced up and was worried about a variety of different things.

What I can say, as actually the email says, is that we did sync up. We were going to, and then I can report that we did sync up on the Red Team results and recommendations and the path forward on the steering committee and other items and his concerns basically were dealt with in a way that was satisfactory to him.

Chairman BROUN. My time is expired. I now recognize Ms. Johnson for five minutes.

Ms. JOHNSON. Thank you very much, Mr. Chairman.

Mr. Park, Mr. Broun summarized your explanation regarding deep dives by saying you had some supervisory responsibilities. Did you indeed have supervisory responsibilities?

Mr. PARK. I would not define it that way. I was an advisor assisting CMS, but CMS was responsible for delivering the Federally Facilitated Marketplace and the new HealthCare.gov.

Ms. JOHNSON. How would you describe your work on HealthCare.gov during your tenure there as CTO?

Mr. PARK. Yes. So we are talking about the new HealthCare.gov, the Federally Facilitated Marketplace. I will again describe it as I referred to in my opening testimony. I assisted CMS in a few different capacities, serving as a co-chair of this interagency steering committee, focused on providing a venue for agencies to work together on interagency issues in support of the hub, assisting with the Red Team exercise and follow-up to the Red Team exercise that summer, serving from time to time as a spokesperson, as a liaison, as someone who could help with particular questions. I began as an assistant, as an advisor to CMS and certainly not as the person who was the hands-on project manager running the thing. I was doing this assistance work as I was fulfilling my much broader portfolio of duties as Technology Policy and Innovation Advisor at the White House.

Ms. JOHNSON. Could you give me a little idea as to what that broader responsibility for being the Chief Technology Officer over and above or around or in conjunction with, in whatever you want to put it, for the dot.gov program for the health care?

Mr. PARK. Yes, ma'am. So as U.S. CTO, my job was to be a technology policy and innovation advisor at the White House focused on how can technological innovation help build a brighter future, create a brighter future for the country and for the American people. So there was a wide range of initiatives that I worked on and championed, so you mentioned one in your opening statement, you mentioned a few, but the open data policy, open data initiatives work of the Administration, which really focused on opening up the information and knowledge in the vaults of the federal government such as weather data, health data, energy data, public safety data, et cetera, as machine-readable fuel that taxpayers had paid for and returning it back to the American people and American entrepreneurs and American innovators and researchers to turn into all kinds of incredible new products, services and companies that help people and that create jobs.

I also was one of the creators and leaders of the Presidential Innovation Fellows program, which was an effort to bring in the most amazing technologists and tech entrepreneurs from outside government and team them up with the best people inside government to work on projects like Blue Button, which has enabled well over 100 million Americans to be able to download copies of their own health information. I did a whole bunch of work in figuring out how we could tap into the ingenuity of the private sector to help use the power of technology to fight the evil of human trafficking, to help improve disaster recovery and response, and other key priorities. I worked on policy issues like how do you advance a free and open Internet, how do you actually massively improve the supply of and utilization of wireless spectrum, and more. It is the most amazing experience I have ever had.

Ms. JOHNSON. It appears to me that though you were a person that could be asked a question or included in a loop that your responsibilities were really very broad and really had no key responsibility toward the HealthCare.gov.

Mr. PARK. So there was a chunk of my time that I reserved for basically being helpful, being an advisor on issues that came up beyond the initiatives that I was championing or co-championing.

That is the bucket in which I put being helpful to CMS on HealthCare.gov, which I did try to do in the capacities that I described.

Ms. JOHNSON. Thank you very much. I yield back, Mr. Chairman.

Chairman BROUN. Thank you, Ms. Johnson. Now I recognize the full Committee chairman, Mr. Smith, for five minutes.

Chairman SMITH. Thank you, Mr. Chairman.

Mr. PARK, thank you for being here today.

Mr. PARK. Thank you, sir.

Chairman SMITH. As I understand it, you were briefed and given notice on several occasions that there were problems with the Obamacare website. So my question is, did you believe that the website was secure when it was first made operational?

Mr. PARK. So I think over the course of any large-scale digital project, there are issues and challenges that come up, so—

Chairman SMITH. Did you think the website was secure before it was operational?

Mr. PARK. I did, sir, to the best of my understanding.

Chairman SMITH. Despite the warnings you got, despite the briefings you had pointing out the problems, you still thought it was secure?

Mr. PARK. My understanding was that it was.

Chairman SMITH. What did you think yourself?

Mr. PARK. Again, I am not an expert.

Chairman SMITH. Did you discount the briefings and the notice that you had gotten?

Mr. PARK. So which briefings and notices are you referring to, sir?

Chairman SMITH. Well, there was a Red Team, there were emails, and then other indications that you knew that there were problems.

Mr. PARK. So the Red Team exercise didn't really focus on security. The Red Team focused on how the project was being run.

Chairman SMITH. The Mackenzie report is what I am talking about that pointed out the problems.

Mr. PARK. Yes, I am referring to the same report, sir. So it didn't really focus on security, it focus on how the project was operating and running generally.

Chairman SMITH. But they still pointed out problems, and you still decided that they were not significant enough, I guess, to put you on notice that it shouldn't be operational?

Mr. PARK. So the Mackenzie report again addressed the general management of the project and talked about—

Chairman SMITH. Again, they pointed out the problems but you discounted the problems?

Mr. PARK. Each of the issues, the risks, was tied to an action to mitigate that risk and deal with that risk.

Chairman SMITH. So you think all the risks were addressed before the website was made operational?

Mr. PARK. I think that the risks identified by the Red Team report, my understanding is that they were addressed.

Chairman SMITH. Well, that is amazing because both then and more recently, all the various studies that were conducted, not a

one found that the website was secure, not a one found that the website was without risk.

More recently, the U.S. Government Accountability Office found “HealthCare.gov had weaknesses when it was first deployed including incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternative processing site to avoid major service disruptions.” This report also finds “weaknesses remain both in the processes used for managing information security and privacy and so forth.”

So you have these outside studies saying that it was not secure at the beginning and it remains insecure. Do you think the website is secure today despite all these warnings by independent, objective entities?

Mr. PARK. So CMS is the best source of information about the detailed security—

Chairman SMITH. Do you discount the Government Accountability Office’s review? The language I just read to you are direct quotes from the GAO.

Mr. PARK. So sir, I am not an expert in this arena. I don’t want to comment on something—

Chairman SMITH. You said repeatedly that you were an advisor. As an advisor, do you advise people that the website is secure today?

Mr. PARK. That is not the area where I really concentrated my advisory work.

Chairman SMITH. Well, knowing what you know now, do you consider the website to be secure today?

Mr. PARK. So based on my understanding, I would use it. I would have family—

Chairman SMITH. No, no, I didn’t ask you whether you would use it. That is easy for you to say yes. Do you think the website is secure today?

Mr. PARK. My understanding is—

Chairman SMITH. Would you advise the American people that the website is secure today?

Mr. PARK. My understanding is that it is, but again, I would say that the best—

Chairman SMITH. Despite the GAO, despite all these studies, despite all these reports saying it is not, you still think it is?

Mr. PARK. The best source of information about that is CMS, and they have a dedicated team—

Chairman SMITH. Well, they are obviously biased. They have got an in-house conflict of interest to say anything else. Do you discount all these third-party entities, these credible organizations saying that it is insecure? Do you disagree with them?

Mr. PARK. Sir, again, I would just refer you to CMS for—

Chairman SMITH. Like I said, you are asking the people that developed the plan whether it is secure. What else are they going to say? I was asking you as an advisor whether you thought these independent entities’ reports were accurate or not.

Mr. PARK. I can’t say that I have actually gone through—

Chairman SMITH. Okay. My last question is this. Did you advise the White House at any point or meet with the White House or brief the White House about Obamacare’s roll-out?

Mr. PARK. Sir, can you repeat the question?

Chairman SMITH. Did you at any point brief the president or the White House about the Obamacare website before it went operational?

Mr. PARK. So as I can recall—

Chairman SMITH. And definitely how many times if you did.

Mr. PARK. As I can recall, I gave a briefing to senior White House officials about the results of the Red Team review and—

Chairman SMITH. How many times did you brief White House personnel?

Mr. PARK. So if you were talking about senior White House advisors—

Chairman SMITH. How many times roughly?

Mr. PARK. I can recall two.

Chairman SMITH. And during either of those times, if two or more times, did you ever say anything to them about the problems that were inherent in the system or about any of the warnings that you had received?

Mr. PARK. So in both the Red Team briefing from early 2013 and then the follow-on in July—

Chairman SMITH. Well, again, my question was fairly specific. Did you alert the White House staff to any problems with the website?

Mr. PARK. So we were very clear, yes, about the risks identified by the—

Chairman SMITH. You did make it clear to the White House that there were risks?

Mr. PARK. That there were risks and here are the actions to mitigate those risks.

Chairman SMITH. But the actions had not been taken yet or that they had been taken yet?

Mr. PARK. Well, the actions at the time we identified the Red Team risks, we presented both the risks and the actions, and then in July we said that the actions had been taken.

Chairman SMITH. Okay. So you notified the White House of the risk and then you came back later and said that you had limited those risks even despite outside entities saying that there were still problems?

Mr. PARK. So this was specifically on how the project was being run, so—and again, just to be super clear, I briefed on the Mackenzie work to senior White House officials that there were risks that needed to be dealt with, and then there were actions that were needing to be taken to mitigate those risks.

Chairman SMITH. Okay. Thank you.

Mr. PARK. —and then—

Chairman SMITH. That answered my question. Thank you, Mr. Park.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Chairman Smith. I now recognize Mr. Peters for five minutes.

Mr. PETERS. Thank you, Mr. Chairman, and thank you for your service on the Committee. It has been a pleasure to serve with you and I wish you the best going forward. Thank you.

There has been some suggestion and some discussion on the security of HealthCare.gov in reference to a hack over the summer, and it is not necessarily true that that means that the site is insecure. HHS worked with the Department of Homeland Security to analyze the effects of the package found on the site, and according to the Director for U.S. Computer Emergency Readiness at DHS, this type of malware is not designed to extract information. There is no indication that any data was compromised as a result of the intrusion.

I would like, Mr. Chairman, unanimous consent to enter into the record a letter from Ms. Tavener to Congressman Issa of November 14, 2014, in which Ms. Tavener states that no one has maliciously accessed personally identifiable information from HealthCare.gov.

Chairman BROUN. Hearing no objection, so ordered.

[The information appears in Appendix II]

Mr. PETERS. Thank you.

Thank you, Mr. Park, for being here. In your testimony, you mentioned that you were not the project manager of HealthCare.gov but you functioned as the project manager for other projects when you were in the private sector. Is that correct?

Mr. PARK. Yes, sir.

Mr. PETERS. Since my colleagues have suggested that you were the project manager of HealthCare.gov or functioned as such, I thought it would be helpful to discuss the kinds of activities that a project manager does. And you founded Athenahealth with Jonathan Bush, incidentally, the cousin of former President George Bush, is that correct?

Mr. PARK. Yes, sir, my best friend.

Mr. PETERS. Athenahealth provides healthcare practices with services including cloud-based medical billing and electronic medical record services, which aims to make healthcare more efficient and effective, correct?

Mr. PARK. Yes, sir.

Mr. PETERS. Since you built the company, can you describe what was involved in creating the company from the ground up? What tasks were involved with developing a new IT company?

Mr. PARK. Thank you, sir.

So as I think others who have had similar experiences would share, you know, it is a big, complex undertaking. You put together the best team that you can. You raise initial money. You put together the best plan you can but understand that that plan is likely to survive about 17 seconds of contact with reality. You put together an initial prototype as fast as you can of your product to try to figure out, you know, based on actual customers using it, what the real issues are and real opportunities are and then you iterate the plan, you iterate the product, you iterate execution constantly, right—

Mr. PETERS. Right.

Mr. PARK. —and it is an all-consuming thing and you have in your head each key axis of effort, how conditions are changing, how plan, product execution are changing constantly—

Mr. PETERS. Is it fair then—

Mr. PARK. —and balance all of that together.

Mr. PETERS. Is it fair then to say when you are on the project management, you are very hands-on? At athena you had a comprehensive, deep understanding of the efforts, very detailed knowledge of the projects and products based on your day-to-day engagement?

Mr. PARK. Absolutely.

Mr. PETERS. Okay. So what is the difference between that role at Athenahealth and the role you played with respect to the healthcare marketplace as CTO and the government?

Mr. PARK. It is night and day, sir, as I think anyone who has built a company or led a large initiative would tell you. I again did advise and assist CMS in a few different capacities, as I described in my testimony and earlier—in testimony and earlier.

The—but again, it is just—it is very different from being the project leader, the project manager, actually running the day-to-day and having the kind of comprehensive, detailed, multi-axis knowledge that you have in that context.

Mr. PETERS. In one of the emails that the Committee has provided, you describe yourself as a consigliere. Is that kind of what you mean, as an advisor?

Mr. PARK. As an advisor, yeah.

Mr. PETERS. Okay. I want to—I do think that—it strikes me that the role of project manager is fairly well-defined as being different from what you were doing. I think that is pretty clear.

I just offer, too, that one of the mistakes we make here in Congress is pulling people out of the bureaucracy and beating them up when we are all really trying to get the same place. We would like to get our government to be functioning—a healthcare website that is functioning. And I am—I would just observe that I have seen this in the Armed Services Committee, too. We are trying to get the best technology people we can to come work for the government, and in the federal—in the defense side we have a great need for cyber warriors and we have to be very sensitive about how we treat people like you and like those folks who can be in the private sector making much more money but who are willing to give up their time, to delay their careers, to step out of them and to help the government.

And I want to thank you for your service. I want you to know that I appreciate it and I hope you are able to help continue to recruit the very, very best to come help us in this effort and other efforts throughout the government.

Thank you, Mr. Chairman, and I yield back.

Mr. PARK. Thank you, sir.

Chairman BROUN. Thank you, Mr. Peters.

Now, I recognize Mr. Sensenbrenner for five minutes.

Mr. SENSENBRENNER. Thank you very much, Mr. Chairman.

Mr. Park, when you testified before the Committee on Oversight and Government Reform, you repeatedly claimed ignorance about any issues with HealthCare.gov prior to the website's launch. You testified that you had "no detailed knowledge base of what actually happened pre-October 1." You further testified that you were not deeply familiar with the development and testing regimen that happened prior to October 1."

But the email record tells a very different story. On June 11, you emailed staff at CMS asking to “check in on how things are going with respect to Marketplace IT development and testing.” On June 26, you said you would visit Henry Chao of CMS and his team for “one of our evening deep-dive sessions,” and on July 12, Henry Chao referenced a briefing that you were doing for the President. If you were preparing to brief the President and doing deep-dives with CMS staff in June and July 2013, how can you claim to have no knowledge of issues prior to October 1 of that year?

Mr. PARK. So thank you for the opportunity to answer your question.

So what I said at the hearing last November was I didn’t have really detailed knowledge—a really detailed knowledge base, if I recall correctly, of what actually happened in the run-up to October 1. And as I have described previously, when I say “really detailed knowledge base of what actually happened,” that is the kind of knowledge that comes from being the hands-on project manager running the thing and not the kind of knowledge that one would have as an assistant advisor who, on a series of occasions, meets with the people who are running the thing and asks questions. So that is what I would say.

Mr. SENSENBRENNER. Well, obviously on the June 11 email, where you said you were going to check in on how things were going with respect to marketplace IT development and testing, you just didn’t ask that question out of the blue. Obviously, you decided to try to check up on this. And then I don’t know what goes on at deep-dive briefings. I imagine that there is quite a bit of detail that goes on. But I guess it kind of boggles my mind that if you didn’t know the detail of that, why were you asked to go and brief the President? Wasn’t he interested in really the detail of what was going on, not just whether it was going well or not?

Mr. PARK. Could you just refer me again to the email you are talking about?

Mr. SENSENBRENNER. Okay. I referred to two emails. You emailed the staff at CMS to check in on how things were going with respect to marketplace IT development and testing, and then on June 26, two weeks and a day later, you said you would visit Henry Chao and his team for an evening deep-dive session.

Mr. PARK. Could you just refer me—I am so sorry—for the tabs in the binder?

Mr. SENSENBRENNER. I don’t know if you have the same binder I have.

Mr. PARK. I see.

Mr. SENSENBRENNER. This is the tab on the deep-dive session, number 8.

Mr. PARK. Okay. So, again, just speaking to this session, the difference between the really detailed knowledge base that you have as a hands-on project manager and the knowledge that you have from asking people on the project a set of questions over the course of a few hours is, again, just night and day.

And also I think to address something you asked earlier, the—as I recall, the trigger event for the check-in that you described was to follow up on the Red Team recommendations with respect to how the project should be managed and make sure those rec-

ommendation had been implemented by CMS. And so that was the trigger event for the inquiry.

Mr. SENSENBRENNER. Well, you denied involvement in your testimony before the OGR Committee, but obviously you were involved because you asked how things were going, then you asked for a deep-dive briefing and you came in to brief the President on this. It seems a complete disconnect between you claiming ignorance and the information you did get filled you in and you certainly weren't ignorant. How can you say that when you came in to brief the President, you briefed him from a base of ignorance?

Mr. PARK. So, again, just to respectfully disagree with something you said earlier, I don't believe I have said—

Mr. SENSENBRENNER. Um-hum.

Mr. PARK. —to the Committee last November that I had no involvement whatsoever. What I said was I didn't have a really detailed knowledge base of what actually happened in response to a question about something or other. So—but, again, the point I wanted to make was that I didn't have that level of really detailed knowledge. I did have the kind of involvement that I described in my testimony earlier.

Mr. SENSENBRENNER. Well, my last question is what did you tell the President about HealthCare.gov when you briefed him?

Mr. PARK. So at the Red Team briefing in early 2013 and then in the follow-up, as I recall, the gist was here are the Red Team recommendations in terms of the risks identified and what to do about them, and then in the follow-up in the summer, as I can recall, the briefing again to senior White House officials was that CMS implemented the key Red Team recommendations.

Mr. SENSENBRENNER. Did you brief the President or senior White House officials or was somebody other than the President there?

Mr. PARK. At those two meetings, as I recall, the President was there.

Mr. SENSENBRENNER. Thank you.

Chairman BROUN. Thank you, Mr. Sensenbrenner.

I now recognize Mr. Cramer for five minutes.

Mr. CRAMER. Thank you, Mr. Chairman, and thank you, Mr. Park.

Mr. Park, I want you to look at tab 5 in the binder if you would, please.

Mr. PARK. Thank you, sir.

Mr. CRAMER. Um-hum. So this is an email that has become a little bit famous today. It is an email from Michelle Snyder to you dated September 29, 2013, posted at 6:22 p.m. In this email, which, by the way, ends by her asking you to delete it, she writes, "just so you know, she decided in January we are going no matter what, hence the really cruel and uncaring march that has occurred since January when she threatened me with a demotion or forced retirement if I didn't take this on. Do you really think she has enough understanding of the risks to fight for a delay? No, and hell no. For just one moment let's be honest with each other."

Now, Mr. Park, it is a reasonable inference that the "she" in the email is Marilyn Tavenner because Ms. Snyder is responding to an email from you to her that same day at 5:54 p.m. that says "MT said that she appreciates the additional info we will generate to-

night, but that she and she alone will make the decision to go or not.”

Mr. Park, what were these risks that Ms. Snyder referenced in her email that she asked you to delete?

Mr. PARK. So at the time what I recall I was doing was helping CMS basically get hardware—additional hardware in place to provide additional server capacity for the federally facilitated marketplace, and that was the issue that we were talking about.

Mr. CRAMER. So the risk was there wasn't enough hardware? In other words, you testified that you thought everything was ready to go, that you were confident. This is September 29. I mean the risk was hardware?

Mr. PARK. So the risks I think that are being referred to in this email is that based on what we had been talking about where I had been asked to be helpful, and the hardware did actually get to where it needed to go in an operation that worked pretty well.

Mr. CRAMER. In this same email chain, about three hours earlier, she asked you this question—which is, by the way, located in tab 6.

Mr. PARK. Oh, thank you, sir.

Mr. CRAMER. Sure. She asked a series of questions, but one of them is “should we go live on October 1?” Now, again, I remind you this is September 29 so she is asking pretty close should we be going live on October 1?

Mr. PARK. I am sorry, who—what—could you just say that one more time? So who is asking who?

Mr. CRAMER. So in—it is the same email chain you asked Ms.—I am sorry, you asked Ms. Snyder a series of questions, one of which is should we go live on October 1. So when you asked her that question, obviously you had some concern it would seem to me earlier that day about whether they should even go live.

Mr. PARK. So, again, as I recall as I am looking at the email, I was suggesting a set of questions for her to think about as an advisor, and again, this was really again focused on the task of getting the hardware in place—

Mr. CRAMER. Did you ask the same question of anyone else? Whether it was Henry Chao or maybe somebody in the White House, Marilyn Tavenner, or was this just between you and Ms. Snyder? Did you raise this question with other people that might be in a position to do something more about it?

Mr. PARK. So I think Michelle was actually, as I recall, pretty central to us, and so I was injecting this set of questions as questions I thought that would be good for CMS to think through in the run-up.

Mr. CRAMER. Some of these risks that Ms. Snyder was raising, did you ever share them? Because clearly there is this confidence, it appears, between you and her. She references in other parts of the rant probably or possibly losing her job if she raises these risks with the wrong people. In fact, she did, of course, announce her resignation not too long after all of this.

What I am trying to get at is that as an advisor, was your advice only given to this one person or to others higher up the chain? I mean considering that earlier you testified that you did of course brief the President himself. Was there other concern raised by

other people to these risks that seem to be so central between you and Ms. Snyder?

Mr. PARK. So with respect to what we are talking about here, which, as I recall, are risks associated with not having enough server capacity the CMS senior management team, Office of Health Reform at the White House were following what was happening very closely.

Mr. CRAMER. And that gave you all the confidence in the world, that extra server space? That was all that was necessary—

Mr. PARK. Well, the specific question that I got asked to be helpful on was getting hardware to the data center for additional server capacity, and that operation did end up being successful as I recall.

Mr. CRAMER. All right. My time is expired, Mr. Chairman. Thank you.

Chairman BROWN. Thank you, Mr. Cramer.

Now, I recognize Mr. Posey for five minutes.

Mr. POSEY. Thank you, Mr. Chairman.

Mr. Park, in an email chain with the subject heading “How serious are you about using Homestead Air Force Base to get the equipment to Culpepper,” this is dated September 28, 2013. It is located in your tab 12.

Mr. PARK. Thank you, sir.

Mr. POSEY. You and Mr. Henry Chao worked with Mrs. Laura Fasching from Verizon Terremark to discuss several last-minute options to transport some hardware or computer equipment by either private ground, private jet, cargo, or even Air Force jets.

For someone claiming to not have a detailed knowledge base of what actually happened pre-October 1, you seem to be all-in on a lot of aspects of operations related to the HealthCare.gov website. So, I am wondering whose idea it was to procure the equipment, and what the need was for spending \$40,000 of taxpayers’ money to transport computer equipment by plane?

Mr. PARK. So, first of all, thank you for the question. Just to clarify, when I say really detailed knowledge base of what actually happened prior to October 1, I am not talking about like one narrow aspect of what happened; I am talking about the full breadth of what happened over the course of the project. And as I have said, I did assist and advise CMS in a few different capacities. This was one where what happened is CMS contacted me, as I can recall, and said we think we have, long story short, a need for additional hardware to get to the data center, and they were the ones who teed up the notion of potentially a military option. And I volunteered to help look into that for them.

Mr. POSEY. Okay. Is it routine for a White House official, or actually, an assistant to the President, as you were at the time, to be engaged in last-minute discussions with a contractor about the delivery of computer equipment? Why and how did you get involved in that?

Mr. PARK. So my style is to try to help in every way I possibly can, and so I got asked to help with this and I threw myself into trying to help. And although the military option ended up not being used; it didn’t have to be used; there was private transport, the operation to get hardware there worked out.

Mr. POSEY. It sounds like a pretty detailed knowledge base.

Mr. PARK. Not of the whole project and how it was working. This is one very specific, very narrow aspect and one episode in time.

Mr. POSEY. You also appear to be the point of contact for most interactions with technology companies and people such as Palantir, Red Hat, Alex Karp, MITRE, and even Gartner, a company used to help with the Administration's messaging on HealthCare.gov around the time of a Committee on Homeland Security hearing on September 11, 2013. In fact, a Gartner analyst provided a quote that the statements made in a CMS letter to the Ranking Member of Homeland Security Committee "represent current best practices for the protection of sensitive and regulated data and systems." That is in tab 14.

Mr. PARK. Oh, thank you, sir.

Mr. POSEY. I am wondering how often did you reach out to such companies or people to talk about aspects of the HealthCare.gov website for either PR purposes or technical purposes?

Mr. PARK. Not that often, as I can recall. But on the several occasions, yes.

Mr. POSEY. And what others do you recall?

Mr. PARK. Well, so you mentioned this one. I can speak to Red Hat. So what happened there was that CMS asked me to be on the phone with them as they asked for additional Red Hat resources to be applied and just to communicate that this was a top priority of the government, which I volunteered to do.

I can talk to the Palantir example. So they are—you know, as part of my role as a facilitator, I connected Palantir to CMS to have a discussion at a high level about cybersecurity.

Mr. POSEY. That is a little bit beyond the scope of advisory, though, wouldn't you think?

Mr. PARK. Not in my experience, no.

Mr. POSEY. Okay. Arranging contractors to get together and—

Mr. PARK. No, we actually—it is assisting, as I have said, in a few different capacities.

Mr. POSEY. What did they have to say about the website? Did they ever provide feedback to you on the security aspects of the website?

Mr. PARK. So as I can recall, the Palantir conversation, I think the experts said here is what you should be thinking about, and CMS said that basically accords with what we are thinking about. So that was what I recall of the call.

Mr. POSEY. And that is the only time you are aware of any security issue at all?

Mr. PARK. Again, and that call basically it was a very high-level call and Palantir said just kind of not with any particular knowledge of HealthCare.gov but here are the kind of things that represent cybersecurity best practices and CMS said, yes, that makes sense; that is what we are thinking, too.

Mr. POSEY. Yeah. You had mentioned that you would use the website. Just out of curiosity, are you enrolled in ObamaCare?

Mr. PARK. I am not but I continue to get my insurance through the Federal Government. But my tour of duty in government, which has been the greatest experience of my life, will at some point end and then I am very excited about enrolling in Covered

California, which is the marketplace in California, when I do roll off.

Mr. POSEY. Yeah. The people who wrote the bill aren't in it either so don't feel bad about that.

My time is expired, Mr. Chairman. Thank you.

Chairman BROUN. Thank you, Mr. Posey.

Now, Mr. Johnson from Ohio, you are recognized for five minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Good morning, Mr. Park.

Mr. PARK. Good morning, sir.

Mr. JOHNSON. You and I share something in common. My background is thirty years in information technology. I have never been a Chief Technical Officer, but I have certainly been a Program Manager, Project Manager, Chief Information Officer, and even had Chief Technical Officers work for me.

Mr. PARK. God bless you.

Mr. JOHNSON. Yeah. So I certainly understand from where you come. And I must confess to you, Mr. Park, that I find it a little bit disingenuous that you would qualify or classify your role in all of this as simply an advisor.

In 2008, when the President issued a position paper on the use of technology in innovation, he talked about standing up the Nation's first Chief Technology Officer. And to quote from what came directly from at that time the campaign website it said that "the CTO will ensure the safety of our networks and will lead an inter-agency effort working with the Chief Technology and Information Officers of each of the Federal agencies to ensure that they use best-in-class technologies and share best practices."

In November of 2008, the President reiterated his intentions, and again quoting from the President-elect's website that he would "appoint the Nation's first Chief Technology Officer to ensure the safety of our networks." Before that, it said "ensuring the security of our networks." So whether you envisioned your role being an advisor, the President said you were responsible. That is what "ensuring" means. As a CIO, and as a Project Manager, I know what "ensuring" means. It was your job to ensure the safety and security of those networks, at least according to what the President was telling the American people.

So I want to go to your role as the co-Chair of the ACA IT Exchange Steering Committee. If I look at the charter that set that up, one of the responsibilities in there is to direct the formulation of workgroups to identify the barriers and recommend fixes and those kind of things, and two of those working groups were directly related to data-sharing and privacy and security harmonization. What was your role then as the co-Chair? You either misrepresented your knowledge of cybersecurity to the President or you didn't do your job. Which was it?

Mr. PARK. So thank you for the opportunity to address I think a couple different questions embedded in there. And I respect your service as technologist, sir, to the country.

So the position of U.S. CTO has evolved quite a lot I think over the years. And what I can represent is what I did in the role, and

cybersecurity ops for the Federal Government has very much not been part of my role.

Mr. JOHNSON. I don't want to use the whole time just pontificating, Mr. Park. When you were with Athenahealth, was cybersecurity a part of what you considered important in standing up that cloud-based system?

Mr. PARK. Sure.

Mr. JOHNSON. It was?

Mr. PARK. Um-hum.

Mr. JOHNSON. Okay. On September the 2nd of 2013, you sent an email to Christopher Jennings. It said, "Hi, Chris. Here are the cybersecurity background points for you. The first three are the points CMS put together previously, which I am sure you have already seen. They are followed by a couple of points about next steps currently underway." So are you trying to tell this Committee that you knew nothing about the security failures and the security risks associated with HealthCare.gov?

Mr. PARK. Would you mind just pointing me to the email that you are referencing? I think it is—

Mr. JOHNSON. I am not sure where it is in your tab, but I have got it here. I don't know where it is in your tab.

Mr. PARK. Well, okay. Let me just speak to the episode that I think you are talking about, but long story short because I know we have very little time left, so the content that was put together for Office of Health Reform on cybersecurity was content supplied by CMS and HHS.

Mr. JOHNSON. But, Mr. Park, there you are being disingenuous again. You are the Nation's CTO appointed by the President to ensure the safety and security of our networks. You can't just say this was CMS's responsibility. And let me remind you that you can delegate responsibility to people that do the actual coding, to Project Managers and Program Managers, but you can't delegate accountability.

Mr. PARK. So again, sir—

Mr. JOHNSON. And you were responsible. You are accountable to the President and to the American people. Now, you have testified this morning that you briefed the President several times. Did you ever once tell the President that you had concerns about the security of the system in your role as Chief Technical Officer and co-Chair?

Mr. PARK. So, again, to go back to I think a fundamental misunderstanding, in my role as U.S. CTO I haven't been—the cybersecurity operations hasn't been a focus—

Mr. JOHNSON. But it was as co-Chair of the Steering Committee. It was clearly in the charter, the co-Chair of the Steering Committee. You did have that responsibility.

Mr. PARK. I was co-Chair on a—one of three co-Chairs on a committee organized by OMB and there was a privacy security subgroup, as you have mentioned.

Mr. JOHNSON. But—

Mr. PARK. That was staffed and led by agency personnel and was really self-propelled and driven by them. The point of us as co-Chairs was to provide a neutral venue where they could get together to do that work.

Mr. JOHNSON. Well, that is not my reading of the charter, but my time has expired, Mr. Chairman, and I will yield back.

Chairman BROUN. Thank you, Mr. Johnson.

Now, I recognize my friend Eric Swalwell for five minutes.

Mr. SWALWELL. Thank you, Mr. Chairman.

I also would like to take a moment to thank you for your service and you served two years as Ranking Member and four years as Chairman of this Committee and you have always conducted yourself and your chairmanship with dignity and courtesy. And I know Mr. Maffei has also shared that with me privately. And so I wanted to thank you for that.

Today may be a day of disagreement but I sincerely believe that if we conduct this hearing fairly, as we have in the past, that we will emerge as a more—we will emerge with a better understanding of what Mr. Park did and, most importantly, did not do with respect to HealthCare.gov.

Fairness is particularly important because this hearing has the feeling quite frankly, as a former prosecutor, of a trial, and the only witness before us is Mr. Park. The title of the hearing implies that we are going to examine his involvement in the development of the HealthCare.gov website, but most significantly, a staff report released by you, Mr. Chair, and Chairman Smith on October 28 functions as a prosecutor's memorandum that makes very damning allegations regarding Mr. Park's honesty before the Committee on Oversight and Government Reform and Dr. Holdren's candor in his replies to this Committee regarding Mr. Park's involvement in cybersecurity. As a former prosecutor, I believe that allegations made against Mr. Park can place him in legal jeopardy. He deserves a chance to tell his own story and put these allegations to rest and I believe he can do that.

Mr. Park is a successful entrepreneur in the IT world who took a break from developing successful companies to come to Washington, D.C., to help the government and the country think of creative ways to use information technology to improve our economy and address important social problems. He is a patriot and he is a son of immigrants who have played their own role in keeping the American economy vibrant and expanding. Mr. Park's parents, I understand, are here today, as is his wife, as is his pastor and friends from the IT business world.

I mention this to remind all Members to not confuse their feelings towards the Affordable Care Act with Mr. Park as a person. He served the public and did his best and should be thanked for his contributions. In fact, Mr. Park has returned to the Bay area, and I know people personally who have been contacted by Mr. Park who he is trying to recruit to bring bright, young, innovative stars to the IT world and to take a break from the multimillion dollar contracts that they have in Silicon Valley, come out to Washington, D.C., and try and solve problems. I cannot imagine that this helps him make that case. In fact, this probably makes it much harder for him to make that case, to go through a process like this.

I have reviewed a minority staff report, which I ask to be made part of the record, built on a complete review of the documents produced by the White House. The staff makes a very strong argument supported by White House documents that Mr. Park did not

have a deep, direct, or intimate involvement in any of the work of developing the online marketplace launched on October 1, 2013, or the cybersecurity standards and techniques used for the site. If he was playing such a role, there should be monthly progress reports from contractors that show progress against deliverables and requirements, costs of work, a critical path analysis that identifies where problems threatened the successful launch, and a discussion of the integration process for the site across an army of contractors on the project.

None of these documents have been produced because Mr. Park was not the day-to-day manager on the project. Nor are there any kind of documents that any of the contractors produce doing the actual work could possess, which would result or include a discussion of code, performance, and testing results. Those documents can be found at CMS, which managed this complex acquisition among the contractors.

I believe that Mr. Park's job was about trying to push technology, and the record and evidence supports that, technology throughout all levels of the country to improve our competitiveness and quality of life. As just one example, Mr. Park drove an initiative to find innovative methods to use IT and big data to combat human trafficking. I don't think there is any Member who favors human trafficking. That is about as nonpartisan as an initiative as you can get. Mr. Park was working full-time in a much wider swath of issues and areas than HealthCare.gov. Members, I hope, will not lose sight of that and get tunnel vision about Mr. Park simply because we have such a narrow set of records.

I believe that if Mr. Park is given a fair chance, a fair opportunity to answer questions here today, that Members on both sides of the aisle will conclude that Mr. Park was not a principal actor in the development of HealthCare.gov prior to October 1, 2013, and had no role in developing cybersecurity standards or techniques for the website.

Mr. Park, I am going to apologize to you now for the way you have been treated and I am hopeful that you will get apologies from the Chairman and other Members by the end of this hearing.

Thank you, Mr. Chair.

Mr. SWALWELL. And, Mr. Chair, I understand that the Chair will yield to me five minutes of questions, which I also appreciate.

Chairman BROWN. And you are recognized for five minutes for questions.

Mr. SWALWELL. Mr. Park, you are not a cybersecurity expert, are you?

Mr. PARK. I am not.

Mr. SWALWELL. Mr. Park, the White House provided several emails from you to CMS relating to cybersecurity. Was there ever a time where you were writing to CMS to give them direction on cybersecurity standards, design, testing, or tools?

Mr. PARK. Not that I can recall, no.

Mr. SWALWELL. When you wrote to CMS, Mr. Park, about cybersecurity, you were doing it because someone at the White House had asked you to gather information, whether for a briefing or meetings or to use as a press event for the White House, is that correct?

Mr. PARK. Correct.

Mr. SWALWELL. When Dr. Holdren wrote to this Committee that “Mr. Park and OSTP personnel have not been substantially involved in developing or implementing the federally facilitated marketplaces security measures;” and “Mr. Park is not a cybersecurity expert. He did not develop or approve the security measures in place to protect the website and he does not manage those responsible for keeping the site safe.” Is every element of the statement made by Dr. Holdren that I just read correct?

Mr. PARK. Yes, sir.

Mr. SWALWELL. Henry Chao ran the website development for CMS and Mr. Chao told the White House—told the House Oversight and Government Reform Committee that he did not run the cybersecurity side of development. With 100 percent confidence do you know before October 2013 who was in charge of cybersecurity on this process?

Mr. PARK. I believe it was Tom Shankweiler, but I am not 100 percent sure he was the leader.

Mr. SWALWELL. Henry Chao, who was doing the day-to-day management of the development of HealthCare.gov, was interviewed by the staff of the House Oversight and Government Reform Committee. He was asked if you Todd Park played a management role and replied that—this is Mr. Chao’s words—you “didn’t own anything meaning he didn’t have the budget, the staff, the contractors, so the day-to-day management really still falls to the operating agencies.” Is this an accurate statement, Mr. Park?

Mr. PARK. Yes, sir.

Mr. SWALWELL. Were you a manager on the HealthCare.gov website?

Mr. PARK. I was not a hands-on project manager, sir, as I have described. I did assist in particular ways that I have testified to earlier.

Mr. SWALWELL. Did you have any control, authority over budgets, staff, or contractors?

Mr. PARK. No, sir.

Mr. SWALWELL. And you asked Mr. Chao about attending the July 19 Readiness Review, which was to be an end-to-end review with all of the contractors about the state of the program. Initially, Mr. Chao said yes. Then you mentioned in an email to Michelle Snyder, Mr. Chao’s supervisor, that you were going to be a “fly on the wall at the event.” And then Ms. Snyder responds that “flies on the wall are seldom invisible and are often distracting.” Then Mr. Chao writes a letter that the review is not the place for an observer. Did you go to this meeting?

Mr. PARK. I do not.

Mr. SWALWELL. You spoke with Mr. Chao and Ms. Snyder about getting a walk-through of the live website system as it was developing in mid-July. People are alleging that you were deeply involved in the implementation and development of the site so I assume that you got that walk-through very quickly?

Mr. PARK. As I recall, I believe the walk-through ended up happening with me and other officials in early September.

Mr. SWALWELL. Now, was that a walk-through that was exclusive to you or were there other officials present?

Mr. PARK. Other officials were present.

Mr. SWALWELL. Those managing or directing multibillion-dollar developmental projects always get a core set of document to track progress. Usually, it is in the form of a monthly report from contractors that show their performance on requirements, the dollars spent, the value achieved, and the critical path issues. Without these detailed reports, Mr. Park, is it possible to have a detailed knowledge of how a project is going at an on-the-ground level? And if so, did you have any reports that would inform you on this?

Mr. PARK. You need those kinds of reports, and frankly, you need more. You need to be on the ground.

Mr. SWALWELL. And were you on the ground?

Mr. PARK. No, sir.

Mr. SWALWELL. Did you have those reports?

Mr. PARK. No, sir.

Mr. SWALWELL. Mr. Chairman, being a spokesperson or collecting talking points for a briefing does not translate into intimate involvement in the development and testing of the website. Mr. Park was not managing the acquisition, he was not directing the development or designing the cybersecurity system, and he sure as heck was not a contractor down in the trenches writing code, which I think is pretty apparent from his testimony. He was the Chief Technology Officer of the United States with the broad portfolio ranging from human trafficking to other important technology advising, and he did a lot more work with that portfolio than any two normal people could pull off. But at some point the actual evidence has to guide our opinion of Mr. Park, which is that he was not intimately involved in the development of HealthCare.gov.

And I yield back.

Chairman BROUN. Thank you, Mr. Swalwell.

And you remind me that, without objection, we will enter in the record our own majority staff report.

[The information appears in Appendix II]

Chairman BROUN. Without objection, the Chair recognizes Ms. Bonamici for five minutes to ask questions.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thank you for allowing me to participate in this Subcommittee hearing. Even though I do not serve on this Subcommittee and do serve on the full Committee, it is an area of interest to me and I am glad to be here today. And I want to thank Mr. Park for being here and withstanding this line of questioning that frankly concerns me. I want to align myself with the remarks made by my colleagues Mr. Peters and Mr. Swalwell.

When we have someone who has come and given so much to this country from the private sector and done so much, we want to make sure that we send a message to the American public that we appreciate your sacrifice and all of your hard work, Mr. Park. And I would imagine that when you said yes when you were asked to come and serve your country, you never imagined that you would be sitting in a Subcommittee hearing with what appears to be a game of gotcha about a whole series of emails.

So I want to start by, again, saying thank you so much for your service. As someone who represents a district in Oregon with a lot of high-tech industry and innovation, I appreciate all you have

been doing and understand that the drive for IT innovation to improve service delivery is something that we can all benefit from, so thank you for your expertise.

Mr. PARK. Thank you, ma'am.

Ms. BONAMICI. You are welcome. And apologies for perhaps being a bit repetitive on some of these issues, but I just want to make sure a couple of things are clear and that is what happens when you go last is that sometimes you sound like you are being repetitive.

But I know that the title on the majority's report says something about "knowingly put Americans' sensitive information at risk." And that is the title of the report. So, Mr. Park, did your interactions with the Administration personnel working on HealthCare.gov give you any cause to worry that they would knowingly put Americans' sensitive information at risk?

Mr. PARK. Not that I can recall, no.

Ms. BONAMICI. Thank you and I understand from the documents that were provided to us by the majority, what we have been looking at here is numerous emails that were exchanged with members of the Administration and officials on the subject of HealthCare.gov, but what we have not seen is what must be many emails that you have exchanged with them on other efforts that occupied your time. I know, for example, that you worked on the ConnectED initiative, and given my role on the Education Committee, I am grateful for your efforts with that as well.

So we heard about a couple of other areas that you worked on but I understand that you oversaw at least 15 initiatives, including HealthCare.gov. So would you care to tell us a little bit about a few of those others just so we can understand the breadth of what you were doing?

Mr. PARK. Sure. And just to be specific, I think the 15 you are referring to, these are initiatives that I was either championing or co-championing. That didn't include HealthCare.gov. Advice and assistance to HealthCare.gov was something I classified into a chunk of my time that was set aside for reacting and helping on issues as they arose.

But in terms of the 15 or so initiatives that I was directly helping to drive, as I described earlier, they included open data initiatives to help unlock the power of the data inside the Federal Government by making it available in machine-readable form for the public so that entrepreneurs and technologists could grab it and turn it into all kinds of incredible services and products and improvement in life and jobs, much as the National Weather Service's release of weather data has really powered all kinds of innovation in weather and jobs as a result.

I championed a set of initiatives, as has been described, to do things like harness the power of private sector technologists and innovators to help fight the evil of human trafficking, rallying innovators to build tools that could help with that. I similarly did the same thing to help improve American disaster recovery and response. I worked on policy initiatives like how to advance a free and open internet, how to actually share wireless spectrum more efficiently and effectively across the country as demand for spectrum continues to increase significantly.

I was a cofounder of the Presidential Innovation Fellows Program that brings in amazing technologists from the private sector to work with the best technologists in government on all kinds of exciting initiatives like Blue Button and Green Button to help Americans get access to their own health data, their own electricity usage data, and more.

Ms. BONAMICI. Well, thank you. And I think we get a sense from that of many of the areas where you do have expertise and where you did serve our country. And I want to suggest that the time on the Science Committee would have been much better spent on talking about some of those issues like open access, like innovation in healthcare technology rather than trying to get you to say that you are an expert on cybersecurity, which obviously from everything that I have read and seen and heard, you are not on this issue.

So thank you again for spending your time here. Thank you for your service. And I hope that we can have you come back sometime and talk about those areas that the public would really be interested in hearing about. That to me, Mr. Chairman, would be a great use of Science Committee time.

Thank you again, Mr. Park, for your service.

Mr. PARK. Thank you, ma'am.

Chairman BROUN. Thank you, Ms. Bonamici. Your time is expired.

Before we adjourn, I would like to give myself some leeway as Chairman of this Subcommittee for the last time with one last question for you, Mr. Park.

Mr. PARK. Yes, sir.

Chairman BROUN. One of your emails provided to the Committee late last Friday was one on October the 10th where you forwarded an article that you had read by David Kennedy, a "white hat" hacker, who has testified twice before this Committee about his concern. And the headline from that article was "Is the Affordable Healthcare Website Secure? Probably Not." Mr. Park, if you want to refer to it, it is in tab 15 in your binder.

Mr. PARK. Thank you, sir.

Chairman BROUN. You even commented about David Kennedy's article that "This got sent to me by someone who says these guys are on the level." Other documents provided to the Committee show that several other cybersecurity experts expressed concerns with the security of the website around that same time. Mr. Park, do you think that David Kennedy's concerns with the security of the website are on the level?

Mr. PARK. So thank you for the question. As I recall, this did get sent to me by someone who thought that TrustedSec was someone that was worth paying attention to. I can't comment on that—

Chairman BROUN. Do you think he is on the level, yes or no?

Mr. PARK. I don't have the judgment—the knowledge of cybersecurity to say and so that is why I forwarded it immediately to CMS, which then evaluated it, and had the response that you see.

Chairman BROUN. Are you being level with us today?

Mr. PARK. Yes, sir. Absolutely.

Chairman BROUN. Okay. According to a news report, it says that you reportedly briefed President Obama, Vice President Biden,

Health Secretary Kathleen Sebelius, and others about the problems with the website only a few days after reading David Kennedy's report. Did you ever express the warnings that were in David Kennedy's report about the lack of security with the website to the President or others in the White House in that October meeting or any other previous meetings?

Mr. PARK. So, again, as I think this email demonstrates, I forwarded this to CMS right away and CMS responded saying CMS acknowledges this feedback by the security committee, analysis—

Chairman BROUN. So just forwarding the email was the only warning that you gave to anyone, is that correct?

Mr. PARK. Well, it says, "Analysis of the code and review of the operational environment has confirmed the site is secure and operating with low risk to consumers," which then got forwarded back to me.

Chairman BROUN. So it is—but that was the only warning you gave anybody, is that correct?

Mr. PARK. Well, sir, again, cybersecurity is handled by CMS, and I think they—

Chairman BROUN. I am just asking. That is a yes-or-no question.

Mr. PARK. So I just—I can report what happened, which is I sent this—

Chairman BROUN. Okay.

Mr. PARK. —asked them to evaluate it—

Chairman BROUN. I take that that—

Mr. PARK. —and got a response.

Chairman BROUN. I take that that the answer is no.

Mr. Park, I want to thank you for finally appearing before this Committee and I am sorry that we had to—

Mr. SWALWELL. Mr. Chairman, may I have a follow-up question, please?

Chairman BROUN. No, sir.

Mr. SWALWELL. Okay.

Chairman BROUN. We have got to adjourn.

Mr. SWALWELL. May I have a follow-up briefly, Mr. Chair?

Chairman BROUN. Mr. Park, I am sorry we came to the point where we had to subpoena you to come before this Committee, but thank you for coming, even possibly under duress.

But obviously people can disagree about whether you were deeply involved or not with the HealthCare.gov website. While I thank you for your government service, the fact remains that the rollout of the HealthCare.gov website last year was a debacle, and that is not my assessment but that of Health Secretary Kathleen Sebelius.

My assessment of this situation remains that you and others in the White House have been neither forthright nor forthcoming about your role and responsibilities at the White House. Integrity in government is integral to the public's faith in our democracy, thus, our Nation's leaders must be open and honest with our fellow Americans and respect the roles of the executive branch and Congress, as articulated in our Constitution.

The fact remains that the White House still has not provided all the documents pursuant to the Committee's subpoena. We have asked for them, we subpoenaed them, we still haven't gotten them.

And perhaps that is why people still disagree about your role in the debacle.

Eternal vigilance is the price we pay for our liberty. To that end, the Committee maintains that all documents pursuant to the subpoena be provided and we ask for the Administration to please provide those expeditiously. After a more thorough assessment of these documents, you may be called to appear before us again, Mr. Park, in order to one day reach a better understanding. While I may no longer be in Congress on that day, the Committee's vigilance on this matter will carry on.

Honest people can fundamentally disagree and we have seen that today. For example, you believe that ObamaCare will be a great thing for Americans, but I think too much of it was predicated on a lie. As a medical doctor, I believe that ObamaCare is the wrong prescription for what ails our nation's healthcare system, but that is a debate for another time.

And with that, I want to thank you, Mr. Park, for appearing before us today, and the Members for their questions. The Members of the Committee may have additional questions for you, Mr. Park, and we will ask that you respond to those in writing, please, and do so expeditiously.

I want to thank my friend Dan Maffei and Eric Swalwell for you all working with me through this process. It has been a great experience for me, and I consider you a friend and consider Dan a friend and I consider all of your staff to be excellent. It has been great working with you all. I had the opportunity to work with Ms. Bonamici also, and I enjoyed working with her, as I told her earlier today. She just left, but it has been a great experience, and I have been tremendously honored by chairing this Subcommittee.

The record will remain open for two weeks for additional comments and written questions from Members. The witness is excused. The hearing is adjourned.

Mr. PARK. Thank you, sir.

[Whereupon, at 11:47 a.m., the Subcommittee was adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Park

Mr. Todd Park, former Chief Technology Officer of the United States,
Office of Science and Technology Policy (OSTP)

**RESPONSES TO QUESTIONS FOR THE RECORD
“The Role of the White House Chief Technology Officer
in the HealthCare.gov Website Debacle.”**

**U.S. House Committee on Science, Space, and Technology
Subcommittee on Oversight**

Wednesday, November 19, 2014

**Questions submitted by House Science, Space, and Technology Committee Chairman Lamar
Smith and Oversight Subcommittee Chairman Paul Broun**

1. **During the early construction and development of HealthCare.gov, including the Federally Funded Marketplace (FFM), were security issues ever raised, and if so, when were you made aware of them, by whom, and did you ever share those concerns with the President or anyone else at the White House?**
 - a. **Given the: (i) risks that were represented in the McKinsey report; (ii) risks that Michelle Snyder mentioned to you in the days leading up to the website; and (iii) the fact that CMS Administrator Marilyn Tavenner was going to make sure that the website launched on October 1, 2013, no matter what (Enclosure 1), at what stage in the development of the website and FFM was security fully implemented in compliance with federal standards?**

Response:

During the early construction and development of the Federally Facilitated Marketplace prior to its launch, I do not recall being made aware of particular problems with the security (i.e., the defenses against malicious cyberattack) of the Marketplace. My recollection of the McKinsey “red team” work in early 2013 was that it focused on how the project to develop the Federally Facilitated Marketplace was being executed in general, focusing on the development of the user-facing consumer experience, and how to improve the management of the project in this regard – as opposed to being focused on security. With respect to Michelle Snyder’s comments in the email chain to which I believe the question is referring, the thrust of that email chain was an effort to bring in additional hardware capacity to reinforce the Marketplace’s ability to support user load, rather than being a discussion about security. CMS is the best source of information regarding the security operations of the Marketplace, including when various certifications were issued in accordance with Federal requirements.

2. **In your deep-dive sessions or status updates of HealthCare.gov, did anyone ever mention that an “end-to-end” test had been performed on the website? Were there ever any concerns about the website’s functionality and security during these meetings? If so, what was conveyed to you and what did you do with that information?**

Response:

In the particular sessions in which I participated prior to the launch of the Federally Facilitated Marketplace, I do not recall whether anyone mentioned that an end-to-end test had been performed. My recollection is that the McKinsey “red team” sessions in which I participated in early 2013 identified risks with respect to general project execution and the development of the user-facing consumer experience and recommended a series of actions to address these risks; this red team exercise did not focus on the cybersecurity defenses of the Marketplace. As discussed in my testimony, the red team’s analysis of project risks and recommended actions to address them were communicated to CMS, HHS, and White House senior leadership, and CMS agreed to adopt the key recommended actions, with the support of HHS and the White House. As with any large undertaking, I remember CMS from time to time explaining challenges they were working through to develop the Marketplace. In particular, I can recall specific open user-facing feature and functionality questions that were raised in discussions and that I worked to help resolve. As examples: I was asked by the White House Office of Health Reform to help assess whether it was feasible to add insurer logos to the display of insurance plans in the Marketplace; after talking with CMS about what such an effort would involve, the opinion I expressed to the Office of Health Reform was that it was not prudent to try to do so during this open enrollment season. I was also asked to assess CMS’s desire to push Spanish-language functionality to a post-October 1, 2013 deployment date; after talking with CMS, my assessment was that this made sense, which I conveyed to White House leadership. As discussed in my testimony, I was also asked by CMS to see if I could help facilitate getting additional hardware transported to the data center hosting the Marketplace in order to provide additional server capacity; I provided assistance as asked; CMS’s progress in this effort was tracked by CMS senior leadership and the White House Office of Health Reform; and my understanding from CMS was that the additional hardware was successfully transported to the data center and brought online.

3. **Where was the quality control on the software development lifecycle and why did Americans see and experience so many issues during the initial rollout?**

Response:

In retrospect, the significant issues experienced by the Federally Facilitated Marketplace at launch reflect fundamental issues with how the Federal Government develops and deploys digital services – issues that have built up over decades and which have resulted in too many government digital service projects performing sub-optimally or worse. It is of vital importance that the Federal Government continue to accelerate efforts to (a) bring more of the best technology talent into government, revamping how we recruit, hire, and train personnel involved in all aspects of the development and operation of digital services for the public; (b) help attract more of the best companies into working with government, companies with strong

competency in modern digital service development approaches and techniques, which have been too often discouraged from competing for government contracts due to the complexity and archaic nature of traditional government procurement practices; and (c) radically revamp the process via which the government develops digital services in accordance with private sector best practices, including the utilization of agile, iterative approaches to software development, best-practice product management techniques, and contracting and budgeting practices that support these.

4. **The following quote comes from your bio previously posted on the OSTP page:**

“In 2013, the President called on Park, a highly accomplished health IT entrepreneur, to help with the successful turnaround of HealthCare.gov. Park, teamed with Jeff Zients, assembled and led the tech surge that overhauled HealthCare.gov, ultimately enabling millions of Americans to sign up for quality, affordable health insurance.”

As part of the effort to improve functionality after the website’s launch, what specific steps did you take relative to the website’s security, including security of people’s personal information?

- a. **What tests did you run on the website to ensure the level of effectiveness of security on the website?**
- b. **Was there ever end-to-end or comprehensive testing done?**
- c. **Did you address what a September 2014 GAO report described as existing weaknesses “in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls?”¹**

Response:

My role in the turnaround of HealthCare.gov and the Federally Facilitated Marketplace post October 1, 2013 focused on helping to reduce the amount of time the site was down, improve the site’s speed, improve its ability to handle high user volume, and improve user-facing functionality (defined as user-facing features and workflow). My work did not focus on the security of the website – which continued to be handled by a dedicated CMS security team; CMS is the best source of information regarding the security operations of the website.

5. **Given your expertise and your involvement with HealthCare.gov, were you surprised to learn that the website was successfully hacked this summer? Do you know or have you**

¹ “HealthCare.gov – Actions Needed to Address Weaknesses in Information Security and Privacy Controls,” GAO, September 16, 2014, available at: <http://www.gao.gov/products/GAO-14-730>. (Emphasis added).

been made aware of any other incidents where personally identifiable information (PII) may have been illegally obtained through HealthCare.gov?

Response:

As context, my knowledge of the incident to which the question refers is second-hand – CMS will have more direct information. As far as I am aware, no personally identifiable information was compromised in the incident. I am not aware of any incidents in which personally identifiable information has been illegally obtained through HealthCare.gov.

6. **As you may know, there is no obligation on the federal government to disclose if Americans' sensitive personal information were breached in a cyber-attack. The House has passed legislation that requires HHS to notify people if their information is stolen from HealthCare.gov. As a former private businessman, HHS CTO and U.S. CTO, do you believe that the federal government should be required to inform Americans whenever their information is compromised from HealthCare.gov, and if so, how quickly?**

Response:

I haven't reviewed the legislation to which this question is referring. With respect to the legislation and this question in general, I would want to seek the opinions of sources such as OMB before forming my own views.

7. **At the November 19, 2014 hearing, you mentioned that you met with the President on at least two occasions regarding the status of HealthCare.gov. How many HealthCare.gov briefings did you actually participate in where the President was present?**
- a. **When was the first time you talked to the President about the security and privacy aspects of HealthCare.gov?**
- b. **Did you ever discuss the operational readiness of HealthCare.gov with the President? If so, when, and what did you tell him about the website's security? Did you discuss any testing that had been done to ensure its readiness?**
- c. **Was there ever a discussion about postponing the launch of the website? If so, did the President ever suggest a delay? Did you ever suggest to the President that he consider delaying the launch of the website?**

Response:

The two meetings on the implementation of the Affordable Care Act that included the President and senior White House leadership that I mentioned in my testimony at the hearing are the only two such meetings in which I can recall participating prior to the launch of the

Federally Facilitated Marketplace. In the first meeting, which was in April 2013, there were multiple presenters, and my role was to talk for approximately ten minutes and summarize the findings of the early 2013 McKinsey “red team” exercise – which identified general project execution and user-facing consumer experience risks and recommended a series of actions to address those risks and improve how the project was operating. In the second meeting, which was in July 2013, my role among the presenters was to discuss, for approximately ten minutes, follow-through on key red team recommendations (CMS agreed to adopt them all, with HHS and White House support) and CMS’s assessment of the current status of efforts to complete the intended functionality of the Marketplace. As I recall, the McKinsey red team exercise’s work did not focus on cybersecurity, and in neither meeting did my talk discuss the site’s cybersecurity defenses. With respect to postponing the launch of the website, I do not recall a discussion considering a delay of the launch of the website at either of those two meetings.

8. **At the Oversight and Government Reform hearing in November, 2013, Rep. Jim Jordan noted that according to White House logs, you attended nine White House meetings run by Ms. Jeanne Lambrew, to which you acknowledged attending meetings from “time to time”² on the subject of the Affordable Care Act. How many of these meetings included discussion of the ACA and HealthCare.gov website, and what was your role in the meetings?**

Response:

Prior to October 1, 2013, I was in meetings run by Jeanne Lambrew from time to time on the subject of the Affordable Care Act. To the best of my recollection, meeting topics included matters related to the development of particular regulations, outreach efforts, and Affordable Care Act implementation. I am not certain how many meetings specifically included discussion of HealthCare.gov and the Federally Facilitated Marketplace, but believe that a number of them did. My role in such meetings was generally to listen to presentations made by others and to offer thoughts and assistance in places where this would be helpful.

9. **Who did you most frequently meet with to discuss the Affordable Care Act and/or the HealthCare.gov website? Who at the White House did you most frequently meet with?**

Response:

Prior to October 1, 2013 (the time period to which I am assuming this question is referring), the people with whom I recall most frequently discussing the Affordable Care Act and/or the Federally Facilitated Marketplace were CMS management (including Michelle Snyder and Henry Chao), the White House Office of Health Reform (including Chris Jennings and Jeanne Lambrew), and the Office of Management and Budget (including Steve VanRoekel).

² “Obamacare Implementation – The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, November 13, 2013, available at: http://oversight.house.gov/wp-content/uploads/2014/06/11-13-13-TRANSCRIPT-Obamacare-Implementation-The-Rollout-of-HealthCare.gov_.pdf. (Hereinafter OGR Transcript).

10. **Did you ever have a conversation about the operational readiness of HealthCare.gov with Dr. John Holdren, OSTP Director? If so, please describe in detail what was discussed?**

Response:

I do not recall having conversations with Dr. Holdren about the operational readiness of HealthCare.gov. I would let Dr. Holdren know from time to time when I was asked to spend time assisting with HealthCare.gov, but I do not recall briefing him in a substantive way about the content of this work.

11. **Referring to Enclosure 2 of this document, did the additional hardware from Verizon that you helped Mr. Chao order in the days leading up to the website launch perform as you expected?**

- a. **Who suggested that additional hardware was needed?**
- b. **Is it typical to order and implement new hardware into a system hours before it is to be released to the public? If not, please explain the risks in doing so?**
- c. **Were you concerned by the need to implement new hardware hours before the website launch? If not, why?**
- d. **Why was the new hardware needed? Please describe the mistakes that lead to the need for this last minute fix.**
- e. **Was the White House made aware of the issues that require this last minute fix? Who informed them?**

Response:

My understanding from CMS, which was the on-the-ground manager of what was happening, was that the additional hardware was successfully transported to the data center hosting the Marketplace and brought online. My recollection is that it was CMS's idea to seek to bring in additional hardware, to add capacity to the system. In my experience, it is not a rare occurrence to add server capacity on rapid timeframes to help increase system capacity. During the work to turn around and improve the Federally Facilitated Marketplace post October 1, 2013, our team added hardware and server capacity on rapid timeframes on multiple occasions – work that does need to be done with care and skill to ensure success. Based on my conversations with CMS management at the time, my understanding of why CMS moved to add more capacity prior to October 1 was due to the need to expand capacity given load testing results and in anticipation of high demand. As I recall, CMS made the White House (including me and the White House Office of Health Reform) aware of this effort. As previously discussed, CMS asked

me to help facilitate getting additional hardware transported to the data center hosting the Marketplace; I provided assistance as asked. CMS's progress in this effort was tracked by CMS senior leadership and the White House Office of Health Reform; my understanding from CMS was that the additional hardware was successfully transported to the data center and brought online.

- 12. Referring to Enclosure 3, in the ACA Exchange IT Steering Committee meeting minutes, it notes that you were engaged in discussion on NIST Level 2 inter-mechanics. Who did you speak with and what was discussed?**

Response:

My recollection is that CMS asked OMB and me—as per the Steering Committee's mission to provide a neutral venue in which agencies could work through interagency items—to facilitate a conversation in which CMS, SSA, and IRS would discuss identity proofing. As part of my role as facilitator, via email and phone, I helped CMS connect with NIST resources (including a NIST employee then on detail to OSTP whom NIST asked to join the conversation), so that CMS could access their expertise on and knowledge of identity proofing and the meaning of NIST Level 2; I am not an expert on such matters. My recollection is that CMS, SSA, and IRS ultimately came to agreement on the topic of identity proofing themselves in a generally self-propelled way.

- 13. Besides the ACA Exchange IT Steering Committee meetings, what other meetings did you attend where the HealthCare.gov website was discussed?**

Response:

In the period prior to October 1, 2013, in addition to the Steering Committee meetings, I attended a variety of meetings at CMS, HHS, and the White House which included discussion of HealthCare.gov and the Federally Facilitated Marketplace (on various aspects of implementation, consumer outreach, and presentation to consumers), including the meetings discussed in my answers to Questions 7 and 8. Other than as described in my answer to Question 7, my role in such meetings was generally to listen to presentations made by others and to offer thoughts and assistance in places where this would be helpful.

14. In an email from Thursday, October 10, 2013, (Enclosure 4) you emailed Marilyn Tavenner an article from TrustedSec and stated, "this got sent to me by someone who says these guys are on the level."

a. Who sent you the TrustedSec article?

b. Did this person email you the article? If so, did they email it to your work or your personal email account?

Response:

On October 10, 2013, Bryan Sivak, the CTO of HHS, sent me the TrustedSec article – via email, to my work account. I sent it to CMS for evaluation. CMS responded shortly thereafter, saying that its analysis and review confirmed that "the site is secure and operating with low risk to consumers."

As a note, in a subsequent conversation in an associated email, on a topic unrelated to the TrustedSec article, I stressed to the Administrator of CMS that it would be important for CMS to conduct thorough load testing and security testing of "Wave D," which referred to new account management software functionality being developed by Marketplace contractor CGI that was potentially going to be deployed to help improve account management performance in the Federally Facilitated Marketplace. I was focused on this effort at the time (early October 2013) because by that time, I was engaged full-time in the HealthCare.gov turnaround effort, working night and day to help address issues, including the ability for users to create accounts and log on to the system; this is why I was writing to the Administrator of CMS on the topic. The new account management software functionality represented by "Wave D" was ultimately not deployed, as an alternate path to account management performance improvement (work dubbed "Wave C+" and subsequent activity pursued by Oracle and others) proved successful.

15. In your testimony before Congress in November 2013, you disagreed with Rep. Jim Jordan's characterization of you as the "head of information technology for the entire United States,"³ stating that you are the "technology and innovation policy advisor in the Office of Science and Technology Policy."⁴

While you were evidently part of OSTP leadership as CTO, and you state in your testimony that you joined "the White House Office of Science and Technology Policy as U.S. CTO," OSTP Administrator John Holdren testified that you did not report to him in testimony he presented before the Committee earlier this year.

- a. What is the role of the U.S. Chief Technology Officer? If it has evolved over time, what changes in responsibilities have been made, and why?
- b. Who did you report to as U.S. CTO? Was the President technically your direct supervisor or was there someone else to whom you reported?
- c. Did you ever brief Dr. Holdren about HealthCare.gov? If so, at whose request, how often, and what did you convey to him?
- d. How did you distinguish between your responsibilities as advisor to the President and as leadership within OSTP? How did the OSTP staff who worked for you make that distinction?
- e. Was your salary as U.S. Chief Technology Officer paid through OSTP?
- f. Did anyone else at OSTP work on aspects of HealthCare.gov (including Presidential Innovation Fellows)? If so, who, and what did they work on?

Response:

My role as U.S. Chief Technology Officer was primarily to serve as an advisor across a broad portfolio of technology and innovation policy issues. I worked on open data policy and initiatives, wireless spectrum policy, how to advance a free and open internet, how to harness the power of technological innovation to fight human trafficking and improve disaster response and recovery, and more. My understanding is that my predecessor, Aneesh Chopra, the first U.S. CTO, also held the title of Associate Director for Technology, which carried with it the responsibility of overseeing Federal investment in technology research. When I assumed the role of U.S. CTO, unlike Mr. Chopra, I did not simultaneously take on the responsibilities of the Associate Director for Technology; this evolution was in order to enable me to devote the desired level of focus on technology and innovation policy. As to earlier conceptions of the U.S. CTO role, I cannot speak to those; I can speak to what I was asked to do in the role.

I was also an Assistant to the President. I took general direction from the White House Office of the Chief of Staff and specific direction from different individuals with whom I would work

³ Ibid.

⁴ Ibid.

on each of the technology and innovation initiatives in which I was involved.

I do not recall briefing Dr. Holdren about HealthCare.gov and the Federally Facilitated Marketplace in substantive ways. I would let Dr. Holdren know from time to time when I was asked to spend time assisting with HealthCare.gov, but do not recall briefing him in a substantive way about the content of this work.

As U.S. CTO and part of OSTP's leadership, I focused on technology and innovation policy, consistent with OSTP's mission. As an Assistant to the President, I held the same rank as Dr. Holdren, and therefore operated as his peer and as a partner, though Dr. Holdren holds overall management responsibility for the operations of OSTP.

OSTP paid my U.S. CTO salary.

With respect to others working in OSTP, other than as specified in my answer to Question 12, my recollection prior to October 2013 is that I would from time to time ask an HHS detailee to attend a HealthCare.gov-related meeting in my stead, to accompany me, or help with some aspect of follow-up work. Post October 1, 2013, I asked a former Presidential Innovation Fellow who was an HHS assignee to help assist the effort to turn around the Federally Facilitated Marketplace.

16. How many Affordable Care Act Steering Committee meetings were held and how many did you attend? How many of these meetings did the other two co-Chairmen attend?

a. Did the Steering Committee stop meeting in early 2013, and if so, why? Did the meetings resume?

b. As co-chairman, what was your role in these meetings?

Response:

The interagency Steering Committee meetings were organized and led by OMB. My recollection is that they were scheduled to occur on an approximately monthly basis. As I recall, I attended a subset of the meetings, but not all of them. I believe that one or both of the co-chairmen from OMB (or their proxies) attended each of the meetings. (Note: one of the co-chairs, Keith Fontenot, left OMB in early 2013.) With respect to my role on the committee, as discussed earlier, my co-chairs and I provided a neutral venue in which agencies could discuss interagency issues, primarily in support of the data services hub, which ended up going live quite successfully.

My recollection is that in early 2013, the interagency Steering Committee moved to a process in which agencies were to ask co-chair and Federal Chief Information Officer Steve VanRoekel to convene a meeting if any interagency issue arose that required it, whenever required, with monthly meeting times held on calendars in case they should be required for such issues. As I recall, this development was spurred by progress agencies had made on interagency issues, the efficiency with which they were collaborating with each other directly, and the desire to

streamline governance mechanisms (a direction reinforced by the McKinsey “red team” exercise). I can recall a couple of interagency calls that happened subsequent to this development, which I do not believe were spurred by any specific issue, but rather were opportunities for agencies to check in on interagency work in general; my recollection was that agencies indicated that their collaboration was going well.

- 17. As of the end of August, 2014, you are no longer the U.S. Chief Technology Officer. However, you are still employed by the Administration.**
- a. **What is your current formal job title and what are your responsibilities, including to whom do you report?**
 - b. **What is your salary and from which office or agency’s budget is it funded?**
 - c. **Does your job position require you to file a public financial disclosure report, and if so, which form(s)?**

Response:

My current formal job title is Consultant. My responsibilities are to help attract more and more of the best tech talent in the Nation to serve in government (which is my current primary focus); to identify innovative ways to improve the quality of government digital services and provide advice on their optimal development and operation; and to help ensure that the Administration has an on-the-ground sense of how technology is evolving and can craft policy and initiatives accordingly. Organizationally, I am located in the White House Office; as a practical matter, I work with and for a wide variety of people and agencies across government, including the United States Digital Service, the White House Office of Presidential Personnel, and agencies seeking key tech leadership. I offered and agreed to not receive compensation in this current role, and I am not required to file a public financial disclosure report.

**Questions Submitted by House Science, Space, and Technology Committee Ranking Member
Eddie Bernice Johnson**

1. In his opening, Chairman Broun said, “We have been waiting a very long time to be able to question you, sir. I am sorry that we had to come to the point of issuing you a subpoena to get that to happen, but I am glad that you are here today, sir.” The Chairman continued, “In fact, the Committee has invited you several times before on five different occasions. We wrote directly to you, Mr. Park, as well as to the Director of the Office of Science and Technology Policy. None of those invitations elicited the “yes” response that we got as a result of issuing you a subpoena.” This introduction created the clear impression that you had been avoiding testifying on the Hill. I would like to give you a chance to address this allegation.
 - a. Isn’t it true that you appeared to testify before the House Committee on Oversight and Government Reform on November 13, 2013?
 - b. The White House sent the Subcommittee a letter (Enclosure 5) on September 16, 2014 offering to provide you to testify for a date in November. Despite this voluntary offer to testify you were given a subpoena to appear. In his closing comments, Chairman Broun said, “I am sorry we came to the point where we had to subpoena you to come before this Committee, but thank you for coming, even possibly under duress.” Was a subpoena necessary to get you to testify before the Subcommittee on Oversight on November 19, 2014? Did you appear under “duress?”

Response:

I did testify before the House Committee on Oversight and Government Reform on November 13, 2013. With respect to appearing before the House Science, Space, and Technology Subcommittee on Oversight, I was prepared to testify before the Subcommittee without a subpoena at a mutually convenient date in November 2014, and offered to do so, as indicated by the letter from the White House that the question references.

2. In his opening statement, Chairman Broun questioned the claims of Dr. Holdren that you were not a cybersecurity expert. He described that “as an interesting description of you to say the least.” He continued, “You are the co-founder of athenahealth, which you co-developed into one of the most innovative health IT companies in the industry and become very wealthy in fact doing that. As a government employee, you helped launch the President’s Smarter IT Delivery Agenda, which created the new U.S. Digital Service, and you created the beta version of Healthcare.gov. How do these activities not require cybersecurity expertise?” The Chairman’s rhetorical question deserves an answer.
 - a. Would you please clarify how you could do all the kinds of things the Chairman references and (still) not be a cybersecurity expert?

- b. Please succinctly explain the kinds of specializations that exist in the IT world that may allow someone successful in one area of IT to not necessarily know very much about another area of IT.
- c. Is it accurate to say that “you created the beta version of Healthcare.gov”, as Chairman Broun asserted? It seems that there is confusion about your work on Healthcare.gov while you were at HHS. Please clarify this matter.

Response:

As someone who has led technology initiatives both in the private sector and in government, I have learned that the key to success is not to try to do everything yourself, but rather, to assemble the best possible team, composed of remarkable people who have expertise in each necessary area, rally them to a common vision, provide the conditions under which they can do their best work, together, and support them in that work. That is what I did at Athenahealth, where in many areas I relied upon the expertise of others. The world of technology, like many fields of professional endeavor, has developed multiple specialties, as opposed to requiring that everyone be equally adept at everything (which as a practical matter is not possible): specialties including various axes of software development, product management, project management, user experience design, data science, site reliability engineering, hardware and infrastructure engineering, cybersecurity, and more.

With respect to the initial version of HealthCare.gov: as articulated in my written testimony for the November 19, 2014 hearing, in August 2009, I was asked to come serve as the U.S. Department of Health and Human Services’ CTO and “entrepreneur-in-residence.” My role at HHS was to serve as a technology policy and innovation advisor. As a special project, after the passage of the Affordable Care Act in March 2010, I was also asked to lead an early effort to develop a website in 90 days that provided basic information about the Affordable Care Act and health coverage options. This website was the first edition of HealthCare.gov, and was a purely informational site; it did not contain a transactional marketplace in which people applied for health insurance. This early website went live very successfully on July 1, 2010. I should note that this website was subsequently essentially completely replaced in 2013 by the Centers for Medicare and Medicaid Services (CMS) with a new HealthCare.gov that incorporated the Federally Facilitated Health Insurance Marketplace.

3. Chairman Smith stated that, “Mr. Park directed several contractors to review the security of the website.”

- a. Did you have the legal or budgetary authority to direct contractors to do any specific work on HealthCare.gov prior to October 1, 2014?
- b. Did you ever “direct” any contractors to review security of the website?

Response:

To my knowledge, I did not have the legal or budgetary authority to direct contractors to do any specific work on the new HealthCare.gov and the Federally Facilitated Marketplace prior to October 1, 2013. I do not recall directing any contractors to review the security of the website.

4. You have described your relationship with Henry Chao and CMS in the development of HealthCare.gov as advisory in nature. The records provided to the Committee reflect that very clearly. However, we do not see similar records between you and Tom Shankweiler, the Chief Information Security Officer at HHS who was directing the security development for HealthCare.gov. Prior to October 1, 2013, how would you characterize your relationship with Mr. Shankweiler?

Response:

Prior to October 1, 2013, I can recall being in meetings where Mr. Shankweiler was also present, but had limited direct interaction with him in general.

5. Mr. Park, Chairman Smith led a line of questioning regarding website risks and security and reports. The end result was that Chairman Smith issued a press release with the header, “Park Admits President Knew in Advance about HealthCare.gov problems.” The text of that release does not elaborate in any way on this claim, or provide a particular quote from you, so it is difficult to know what “problems” the Chairman believes the President may have known of from your briefings. However, the claim is clearly rooted in Chairman Smith’s questioning. The Chairman made reference to the Red Team evaluation exercise you participated in and the Mackenzie report, and seemed to suggest that you should have known prior to October 1, 2013 the results of a Government Accountability Office report on cybersecurity of the website that was not available until the Summer of 2014. You did acknowledge briefing senior officials in the White House about the risks identified in the Red Team and Mackenzie reports.

- a. Can you succinctly summarize the Red Team and Mackenzie report “risks” and, to the degree you know, briefly describe the actions that were taken to address those risks? Be very clear about which of these risk evaluations, if any, were about cybersecurity.

- b. You mention that you believed there were two briefings for White House senior leadership where the President was in attendance. To the best of your recollection, how many briefings involved the President and when did these occur?**

Response:

The McKinsey “red team” exercise in early 2013 identified both key risks to the Marketplace’s user-facing consumer experience and recommended actions to address those risks, which CMS agreed to adopt, with HHS and White House support. For instance, to address the risk that the Marketplace and Hub would be unavailable due to system failure, the exercise recommended prioritizing and locking down remaining open requirements for version 1.0 of the Marketplace with rapidity, maximizing time for testing, and establishing an operations command center and response capability to deal with post-launch issues. To mitigate the risk that the Federal Marketplace would not be able to absorb large-volume State-based Marketplaces (e.g., NY, CA) at the last minute should those states run into blockers, the exercise recommended communicating with states that they needed to make definitive decisions by a near-term deadline about whether they were going to continue with State-based Marketplaces or go the Federal route. To the best of my recollection and knowledge, none of these key risk evaluations were focused on assessing the cybersecurity defenses of the Marketplace.

With respect to briefings prior to October 1, 2013, with White House senior leadership where the President was in attendance, as referenced in the question, I can recall attending two such briefings – the first in April 2013 and the second in July 2013.

- 6. At times during the hearing, Majority Members used your detailed knowledge about a single, specific matter—for example the effort to get more server capacity on line for October 1—to assert that because you knew that matter so well you must have had detailed knowledge of the project across the board. Please explain again how your role as an advisor for HealthCare.gov put you in a position where you would have detailed knowledge about a specific issue, but still not be in a position to have the kind of detailed information that a day-to-day project manager would have?**

Response:

As I discussed in my testimony, I was not a project manager who was managing and executing the day-in and day-out operational work of building the new HealthCare.gov and the Federally Facilitated Marketplace. This was the responsibility of CMS. I did not have the kind of comprehensive, deep, detailed knowledge of the effort that a hands-on project manager would have, and which I have had about other projects in my private sector work. Prior to October 1, 2013, I assisted CMS with its work in a few different capacities as an advisor, as described in my testimony, while executing my overall duties as White House technology policy and innovation advisor, working on a broad range of policy and innovation matters ranging from open data to fighting human trafficking. With respect to the assistance I provided to CMS, on a particular issue on which my assistance was requested, I would garner particular knowledge on that specific issue at that moment in time; however, I did not have the kind of detailed,

across-the-board, ongoing knowledge of the project that a day-to-day, on-the-ground project manager would have.

7. **Mr. Johnson made reference to a campaign position advocated by then-candidate (or President-elect) Obama in which it was proposed that a Chief Technology Officer position would be created and, among the examples of their mission said that a CTO would “ensure the safety of our networks” and to ensure the “security of our networks.” Mr. Johnson then made a series of statements that took that proposal from 2008 as a factual statement of your responsibility as CTO. Never were you asked directly if establishing agency-wide cybersecurity standards was included in your portfolio when you came to the CTO job in 2012. Nor did Mr. Johnson mention that the 2002 E-Government Act actually created an office at OMB, the administrator of the Office of Electronic Government (and the two most recent occupants of this position have taken on the title of Chief Information Officer) with responsibility for many aspects of interagency IT policy, including ensuring computer architecture security across the government.**
- a. **When you came to the CTO job in March, 2012, were you tasked by the President with ensuring the safety and security of Federal computer networks?**
 - b. **Based on your experience, was it the CJO at OMB who was charged with interagency cybersecurity responsibilities?**

Response:

When I came to the U.S. CTO job in March 2012, I was not tasked by the President with ensuring the safety and security of Federal computer networks. It is my understanding that it was the CIO at OMB who was charged with interagency cybersecurity responsibilities.

8. **Mr. Cramer asked you about an email exchange with Ms. Snyder on September 29, 2013. I would like to give you a chance to lay out the context of this email--you mentioned hardware issues during the hearing--and how that was resolved?**

Response:

As I recall, the thrust of the email chain was an effort to bring in additional hardware capacity to reinforce the Marketplace’s ability to support user load. Based on my conversations with CMS management at the time, my understanding of why CMS was moving to add more capacity prior to October 1 was due to the need to expand capacity given load testing results and in anticipation of high demand. CMS asked me to help facilitate getting additional hardware transported to the data center hosting the Marketplace in order to provide additional server capacity; I provided assistance as asked. As discussed earlier, my understanding from CMS was that the additional hardware was successfully transported to the data center and brought online.

9. **Compare and contrast your involvement in HealthCare.gov before and after October 1, 2013.**

Response:

With respect to the new HealthCare.gov and the Federally Facilitated Marketplace that launched on October 1, 2013: prior to the launch, I assisted CMS with its work in a few different capacities as an advisor, as described in my testimony, while executing my overall duties as White House technology policy and innovation advisor, working on a broad range of policy and innovation matters ranging from open data to the fight against human trafficking. After the launch, as the extent of the operational issues with the site became clear, it became an all-hands on deck moment, and I, along with others, dropped everything else I was doing and increased my involvement in HealthCare.gov dramatically, shifting full-time into the HealthCare.gov turnaround effort, and working as part of the “tech surge” that radically improved the performance of the site. I worked as part of a terrific team, working around the clock, even sleeping on office floors. My particular focus was on helping to reduce the amount of time the site was down, improve the site’s speed, improve its ability to handle high user volume, and improve user-facing functionality. Our team effort drove massive improvement in the site, ultimately enabling millions of Americans to successfully sign up for health insurance through the site.

Enclosure 1

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Sunday, September 29, 2013 6:22 PM
To: Park, Todd
Subject: Re: Discussion points

Just so you know she decided in January we were going no matter what - hence the really cruel and uncaring march that has occurred since January when she threatened me with a demotion or forced retirement if I didn't take this on - do you really think she has enough understanding of the risks to fight for a delay - no and hell no - for just one moment let's be honest with each other. I appreciate you belief in the goodness of others but at this point I am too tired to pretend there is a decision to be made - it is just how much crap my team will have to take if it isn't sufficiently successful - you haven't lived through the temper tantrums and threats for the last 9 months.

OK - that felt good - am now back to my role as no comment civil servant

Delete this after reading - promise

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 05:54 PM
To: Snyder, Michelle (CMS/OA)
Subject: RE: Discussion points

Yes, got it. On the call with MT, Chris, and Jeanne, MT said that she appreciates the additional info we will generate tonight, but that she and she alone will make the decision to go or not - which of course is right. And the way she is thinking about it from a performance standpoint is that if enough of the additional hardware gets online to give us an insurance policy, she is comfortable proceeding, with 90,000 concurrent users being far beyond the 50,000 that was the CMS target.

Because new hardware is going live on a rolling basis today and tomorrow, I think we are in very good shape on the hardware front -- and because the Miami equipment got here so early today, we've got a good shot at that being live and helping us get to 90,000.

Will be good tonight as per one of the questions for the 9 pm to get people's guesstimate of what kind of traffic in general (order of magnitude) would be associated with a 90,000 concurrent user scenario, just so MT has that.

And will also be good to understand the EIDM situation a bit better to see if that is a separate bottleneck with a lower concurrent user threshold? And if that's a possible threat to monitor. Again, just to inform MT.

Going to deliver cupcakes now :)

-----Original Message-----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]

Enclosure 2

From: Fasching, Laura <[redacted]>
Sent: Saturday, September 28, 2013 10:47 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Glad to help, let me know if you need anything else gentlemen ☺
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [redacted]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[redacted]]
Sent: Saturday, September 28, 2013 10:38 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

That is super-awesome! Laura, thanks so very, very, very much!!!!

From: Fasching, Laura [mailto:[redacted]]
Sent: Saturday, September 28, 2013 10:36 PM
To: Chao, Henry (CMS/OIS); Park, Todd
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd & Henry,

The shipper is picking up the equipment in the next 90 minutes from the Miami data center and we expect the shipment to arrive between 9:30 AM to 10:00 AM. ☺

So Monday COB is looking good as long as we keep the shippers on schedule, as the build teams will be working at 5 am with the equipment that was brought in today.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [redacted]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Chao, Henry (CMS/OIS) [mailto:[redacted]]
Sent: Saturday, September 28, 2013 9:03 PM
To: Fasching, Laura; Todd Y Park [redacted]
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

I got the approval from our COO and head of Contracts to go with the 40k option.

Contracts said we will have to work out how this can be a line you can bill in the contract but no problem figuring that out later.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[Redacted] (Pri)
[Redacted] (Alt)
[Redacted] (BB)

From: Fasching, Laura [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 09:00 PM
To: Park, Todd <[Redacted]>; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura <[Redacted]>
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Ok great Henry can I get confirmation that the Government will pay for the plane? We have to get David Small's approval so we will need to call him as soon as possible.

Thanks and sorry to rush you all.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon TerraMark
Tel: [Redacted]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 8:50 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

FYI, the private plane option I am pursuing would likely cost about the same as the Fedex expedite cargo plane option below.

Henry, I think that delivery to the data center mid-day Sunday sounds really, really, really good...

From: Fasching, Laura [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 8:46 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?
Importance: High

Ok here is what I was able to do
I was able to get to FedEx custom Critical they can drive it to us via a truck with pick up tonight @ 11:00 PM (ish) and delivery around 9 PM on Sunday night for \$3700.00
Or

To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Laura, by when do you need to make a decision about whether to send via private ground, private cargo plane, or Air Force (if Air Force is indeed an option?)

And to confirm private ground would deliver the hardware on Tuesday (to be installed Wednesday?), private cargo plane would deliver the hardware on Monday (to be installed Tuesday?). With no possibility of acceleration of those timetables?

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Saturday, September 28, 2013 7:29 PM
To: 'laura.fasching'; Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd--it's in your hands now to make a quick decision.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

(Pri)
(Alt)
(BB)

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 07:27 PM
To: Park, Todd < >; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

We have been exploring that option too but no luck so far

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [redacted]
222 W Las Colinas Blvd, Irving, Texas, 76039

From: Park, Todd [mailto:]
Sent: Saturday, September 28, 2013 7:26 PM
To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Also: as another option to explore, in the interest of exploring all options simultaneously, is it possible to arrange for heroic chartered private sector ground transportation that could get going super-early tomorrow morning and get to Culpeper by Sunday evening?

From: Park, Todd
Sent: Saturday, September 28, 2013 7:03 PM

To: 'Chao, Henry (CMS/OIS)'; laura.fasching [REDACTED]
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

WH team responded instantly, is working on it as we speak and will get back to us ASAP. But they unfortunately are not optimistic, so we should explore other options in parallel.

Is there any possibility of arranging for private/commercial cargo plane transport? Chartered, even?

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 6:36 PM
To: 'laura.fasching' [mailto:[REDACTED]]
Cc: Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Just talked to Todd and he is going to talk to the rest of WH that can make this happen so just reply with the confirmed service to Homestead.

Todd--let us know ASAP so Laura will send via ground if you can't arrange for transport to someplace the Air Force can land near Culpeper VA.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[REDACTED] (P)
[REDACTED] (A)
[REDACTED] (B)

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 06:09 PM
To: Chao, Henry (CMS/OIS)
Cc: Fasching, Laura <[REDACTED]>
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Henry,

We are working on firming up the white glove shippers but once that is done we would be good to go.

If we get the shippers scheduled and the equipment gets here tomorrow my engineers said they have the resources to build it out and just like we said before up by cob Monday.

I will let you know about the shippers within an hour.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon TerraMark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

Enclosure 3

Key Points Discussed		
No.	Topic	Highlights
2	Workgroup Updates	<p>dependencies from consent.</p> <p>Marilyn Tavener has been engaged in the consent resolution conversations.</p> <ul style="list-style-type: none"> • Details cannot be flushed out until these conversations are complete. • CMS has been ordered to await the completion of these discussions before determining the necessary changes to the baseline schedule. <p>Todd Park has been engaged in discussion on NIST Level 2 inter-mechanics.</p> <ul style="list-style-type: none"> • CMS is moving forward with following this process, which represents SSA's understanding, as well. • SSA is interested in understanding the downstream impact on the overall integrated testing, as well as the timeline. <p>Scheduling</p> <ul style="list-style-type: none"> • Highest risk to implementation associated with awaiting the high-level decision, as opposed to building for the worst case scenario: <ul style="list-style-type: none"> ○ Broad risk: Schedule and implementation risks would be the largest concerns. The schedule presents a risk of a 2-4 week delay. ○ The team must agree that the schedule risk is a priority and must find ways to retrieve the lost time from other areas. ○ It is unclear as to whom the Secretary is in discussion with or what the status of the discussion is. ○ Teams thought there would be simultaneous development between the legal issue and the IT build as the higher level issues were being addressed. The interagency team is not in full agreement on this issue. ○ David Black would like the teams to continue making technology progress. <p>Clarification: Identification Proofing vs. Consent</p> <ul style="list-style-type: none"> • Consent is a legal issue, whereas, identity proofing is a solution and process that needs to be established. • SSA is relying on the Privacy Act for legal authority on ID proofing as there is none provided in the Act. <ul style="list-style-type: none"> ○ Legal team is currently working this issue. ○ Identity proofing would be built in as a process for verifying an individual's identity. • Previous decision to use two IRS challenge questions at the threshold has been reconsidered and is currently being discussed. • Suggestion: A smaller group of key individuals may need to reconvene on this topic in 3-4 weeks including Marilyn because of her involvement with the scheduling. <p>Integrated Project Plan</p> <ul style="list-style-type: none"> • The IPP needs to be addressed before focusing on the schedule

Enclosure 4

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Thursday, October 10, 2013 5:03 PM
To: Park, Todd
Subject: FW: Item

A.Michelle Snyder
 Chief Operating Officer
 DHHS/CMS/OA
 [REDACTED]

From: Trenkle, Tony (CMS/OIS)
Sent: Thursday, October 10, 2013 4:54 PM
To: Snyder, Michelle (CMS/OA); Tavener, Marilyn (CMS/OA); Kerr, James T. (CMS/CMHPO)
Subject: RE: Item

Here's the answer below, maybe more detail than you want.

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, October 10, 2013 2:08 PM
To: Fryer, Teresa M. (CMS/OIS)
Cc: Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS)
Subject: RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

Statement:

CMS (CIISG) acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the java script posted on-line. The code base at CGI has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The XOC Security team and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform JS comment-removal/minification/obfuscation is a roadmap item, in fact it is scheduled for release to the Test2 environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during YUI compression. As java scripts can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a

consumer as A Good Consumer Experience was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP
Information Security Officer, CCHIO
CMS\OIS\CHISG
Consumer Information and Insurance Systems Group
[Redacted] (Balt. Office, N2-13-22)
[Redacted] (Mobile)

From: Snyder, Michelle (CMS/OA)
Sent: Thursday, October 10, 2013 4:41 PM
To: Trenkle, Tony (CMS/OIS)
Subject: Fw: Item

Could you take a look?

Sent from my BlackBerry Wireless Device

From: Tavenner, Marilyn (CMS/OA)
Sent: Thursday, October 10, 2013 04:10 PM
To: Snyder, Michelle (CMS/OA); Kerr, James T. (CMS/CMHPO)
Subject: FW: Item

Wanted you to have this in case you want to have tony reach out to them

From: Park, Todd [mailto:[Redacted]]
Sent: Thursday, October 10, 2013 2:11 PM
To: Tavenner, Marilyn (CMS/OA)
Subject: Item

Marilyn, this got sent to me by someone who says these guys are on the level. I would suggest that the Marketplace IT security folks check it out (and potentially reach out to these guys as well)

https://www.trustedsec.com/october_2013/affordable_health_care_website_secure_probably/

Enclosure 5

THE WHITE HOUSE
WASHINGTON

September 16, 2014

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Broun:

I understand that last Friday the Committee on Science, Space, and Technology's Subcommittee on Oversight (the Subcommittee) noticed a September 17, 2014, business meeting to consider issuing two subpoenas. As described in the notice, the Subcommittee will consider whether to issue a subpoena for Todd Park to appear at a hearing before the Subcommittee, and whether to issue a subpoena for the production of some of Mr. Park's records, during his former tenure in the Office of Science and Technology Policy (OSTP) as United States Chief Technology Officer (CTO), relating to the healthcare.gov website.

I write in advance of the Subcommittee's meeting to ensure you understand that the issuance of these subpoenas is unnecessary. Mr. Park will appear voluntarily for a hearing before the Subcommittee on a mutually convenient date in November to discuss your expressed interest in the healthcare.gov website. OSTP is willing to produce additional documents—including the 102 pages proactively provided with this letter—to further accommodate your efforts to examine the safety, security and privacy of Americans' personal data through the [Obamacare](http://Obamacare.gov) website.¹ The remainder of this letter discusses OSTP's efforts to cooperate with your oversight interests thus far, and OSTP's continued willingness to do so without any need for subpoenas.

I understand that both the full Committee and the Oversight Subcommittee have articulated their interest in the security of healthcare.gov as a desire for information about the measures in place to defend the healthcare.gov website against malicious cyber attacks and to safeguard the personal data of Americans. When Chairman Smith initially wrote to Mr. Park to express interest in healthcare.gov, the letter asked Mr. Park to address "what specific security standards and technical measures are in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or

¹ Letter from the Hon. Lamar Smith, Paul Broun, M.D., and Lary Bueshon, M.D., to the Hon. John P. Holdren, Director, Office of Science and Technology Policy (December 20, 2013) [hereinafter "December 20 Letter"], at 3.

leaked.² An email from Committee staff to OSTP at about the same time expressed interest in cybersecurity issues more generally, including a cybersecurity policy report that OSTP Associate Director Patricia Falcone helped prepare.³ In the same vein, your December 20, 2013, letter to OSTP referenced a hearing the Committee held in November of that year to examine the risks that online criminals and identity thieves might pose if they gained access to customers' personal information.⁴ And more recently in January of this year, the Committee continued its focus on the standards and technical protocols in place to defend against malicious cyber attacks in a second hearing convened on the same topic with "white hat" hackers as witnesses.⁵

From the outset, OSTP has been clear about the limitations both it and Mr. Park face in attempting to respond to the requests for information and testimony concerning these issues involving the development of security standards and the design of scenarios to respond to malicious intrusion attempts. As noted several times in prior correspondence, primary responsibility for those tasks lies elsewhere—with the Centers for Medicare and Medicaid Services (CMS)—and it is CMS that is in the best position to provide complete, current, and accurate information regarding the security protocols in place to protect the website. Nevertheless, the record reflects that OSTP has made substantial efforts to try to accommodate the Committee's interest in security and to clarify Mr. Park's role.

OSTP has produced more than one thousand pages of documents; offered on multiple occasions to have Associate Director Falcone testify at a Committee hearing on cybersecurity policy issues; made Mr. Park available for a meeting with you and Chairman Smith in your office, where Mr. Park was willing to address any questions put to him; and offered to have Mr. Park brief all Subcommittee members. Through these substantial efforts at accommodation, OSTP has attempted to help the Committee better understand Mr. Park's actual duties as the United States CTO and his role with respect to healthcare.gov.

In particular, regarding the documents you have received, your letter of December 20 asked OSTP to produce a very broad set of materials, including all OSTP records concerning the Affordable Care Act and healthcare.gov, scheduling information, records concerning internal White House briefings, and even documents that had not been created but might conceivably be provided to Congress in the future.⁶ Confronted with this broad request and a short deadline in the December 20 letter for responding, OSTP focused its efforts to provide information on the issue that was plainly of particular interest to the Committee, namely, Mr. Park's participation as one of three co-chairs on the healthcare.gov Interagency Steering Committee. Your December

² Letter from the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology, to Todd Park, Assistant to the President and United States CTO (October 31, 2013), at 1.

³ Email from H. Comm. on Science, Space, & Technology Majority Staff to OSTP staff (Oct. 28, 2013, 5:42 p.m.) ("I suspect we would touch on related issues raised and addressed in the 'Cyberspace Policy Review' and the Dec 2011 report 'Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,' both of which were referred to in Dr. Holdren's testimony before the Committee in a full committee oversight hearing on June 20, 2012.")

⁴ December 20 Letter, at 1 ("The expert witnesses at our hearing outlined the significant risk of identity theft to Americans if hackers gained access to their personal information.")

⁵ *Hearing Before the H. Comm. on Science, Space, & Tech.*, 113th Cong. (January 16, 2014) [hereinafter, January 16 Hearing].

⁶ December 20 Letter at 3.

20 letter focused on this Steering Committee and its security and privacy subgroup—even going so far as to attach a draft charter for the Steering Committee.⁷

Accordingly, in its January 15, 2014, response, OSTP described the documents it was producing: those concerning the Steering Committee and other interagency meetings that made reference to security, which appeared to be of special interest to the Committee.⁸ OSTP's January 15 letter also explained the interagency coordination function the Steering Committee served, Mr. Park's role in it, and why his participation was not an indication that he had substantial knowledge or expertise concerning the standards or technical protocols for dealing with malicious intrusions that are the focus of the Subcommittee's oversight inquiry. In the eight months following OSTP's production of these documents, the Subcommittee expressed no continued interest in receiving additional documents, nor did it raise any questions concerning the Steering Committee materials provided. Thus, you can understand why the abrupt notice of a business meeting to consider a subpoena for documents came as a surprise.

Despite OSTP's efforts at accommodation, it seems that the push to issue subpoenas this fall may unfortunately reflect a continued misunderstanding of Mr. Park's involvement in the security of the healthcare.gov website. This letter therefore provides additional information, namely, additional OSTP documents beyond those already provided concerning the Interagency Steering Committee, concerning Mr. Park's limited involvement in the security aspects of the website, which are primarily handled by CMS. The enclosed documents can be grouped into three categories.

First, in an extension of his role with the Steering Committee, Mr. Park, and his other co-Chairs were occasionally asked to assist in instances when White House personnel made requests to officials at HHS and CMS. One instance when such assistance was sought involved a request for a meeting on user credentialing and identity-proofing from National Security Staff and Office of Management and Budget officials. The documents themselves make clear that although the particular request for assistance was made from CMS officials to Mr. Park, it was another co-Chair who provided assistance in addressing that request.⁹

Second, Mr. Park was asked on a small number of occasions to assist in obtaining information from CMS and HHS personnel responsible for security of the website. In that role, Mr. Park asked HHS and CMS officials to develop background points describing the cybersecurity protections and helped coordinate follow-up conversations between the HHS and CMS officials and cybersecurity experts both inside and outside the government. Again, the emails themselves show that Mr. Park was not directly familiar with the development of

⁷ See also *January 16 Hearing* (statement of Rep. Paul Brown, M.D.) ("It's probably [sic] the oversight committee of—subcommittee of this committee's attention that there is—or at least was [an] Affordable Care Act information technology exchanges steering committee [chaired] by senior White House officials established back in May 2012, almost a year and a half before the roll out of Healthcare.gov.").

⁸ Letter from the Donna Pignatelli, Director, OSTP Legislative Affairs, to the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology (January 15, 2014) [hereinafter January 15 Letter], at 3. At Chairman Smith's request, OSTP also produced all documents that it had at that point provided to the Committee on Oversight and Government Reform.

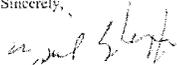
⁹ Email from Steven VanRoekel to J. Michael Daniel, et al. (Apr. 12, 2013, 3:25 p.m.), enclosed.

cybersecurity defenses in place, but instead served as an intermediary and relied on the HHS and CMS officials to provide the substance of the information he then passed on to others.¹⁰

Third, shortly before the first open enrollment period, Mr. Park also served as a liaison with cybersecurity officials at HHS and CMS in connection with efforts to explain publicly the cybersecurity protections for the health insurance marketplaces. This "spokesman" function is one Mr. Park performed from time to time as CTO with respect to technology issues generally. Importantly, the enclosed emails again confirm that Mr. Park was not speaking from direct personal knowledge or experience on cybersecurity—before participating in a press call, he solicited the relevant information from CMS cybersecurity personnel and sought to have them participate in the call given his relative lack of familiarity with cybersecurity issues.¹¹

The information provided in and with this letter is consistent with what OSTP has previously explained: that CMS is best positioned to address the Subcommittee's questions regarding the security of the website and that Mr. Park has not been substantially involved in developing or managing the "specific security standards and technical measures . . . in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website . . ." More importantly, if the Subcommittee desires additional information, there is no need to resort to subpoenas. Mr. Park will be pleased to testify at a Subcommittee hearing in November. OSTP is also actively searching for additional records that may further illuminate Mr. Park's relatively minor role on cybersecurity issues and is willing to voluntarily produce additional documents to aid the Subcommittee's inquiry. Please simply have your staff communicate the Subcommittee's priorities in that regard to OSTP.

Sincerely,



W. Neil Eggleston
Counsel to the President

¹⁰ Email from Todd Park to Tony Trenkle, et al. (Sept. 2, 2013, 1:14 p.m.), enclosed ("Hi Tony, many apologies for interrupting your Labor Day, but can you help Chris with his follow-up question below (reference to 'current federal standards and how they exceed private sector as well as track record of protection from attacks').").

¹¹ Email from Todd Park to Tony Trenkle, et al. (Sept. 17, 2013, 9:54 p.m.), enclosed ("I've let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can talk to it at a general level only -- she thinks that will be OK on the call tomorrow, with detailed questions to be referred to agencies.")

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD

WRITTEN STATEMENT SUBMITTED BY REP. ERIC SWALWELL

Mr. Chairman, first, I would like to take a moment to thank you for your service. You served two years as Ranking Member and four years as Chairman. During your tenure, you have always conducted your chairmanship with generosity and great courtesy. While we have not always seen eye-to-eye on the matters before the Subcommittee, no Member on this side of the aisle has ever had reason to complain about the way you have conducted yourself, and that has gone a long way towards keeping relations civil and even cordial in the midst of disagreement. Thank you.

Today may be a day of disagreement, but I sincerely believe that if you conduct this hearing as fairly as you have your past hearings, that we will all emerge with a clear understanding of what Mr. Park did and did not do related to HealthCare.gov.

Fairness is particularly important because this hearing has the feel of a trial. The only witness before us is Mr. Park. The title of the hearing implies that we are going to examine his involvement in the development of the Healthcare.gov website. Most significantly, a staff report released by you and Chairman Smith on October 28 functions as a prosecutor's memorandum that makes very damning allegations regarding Mr. Park's honesty before the Committee on Oversight and Government Reform and Dr. Holdren's candor in his replies to this Committee regarding Mr. Park's involvement in cybersecurity. As a former prosecutor, I believe that the allegations you have made against Mr. Park could place him in legal jeopardy. He deserves a chance to tell his story and put these allegations to rest, and I believe he can do that.

Mr. Park is a successful entrepreneur in the IT world who took a break from developing successful companies to come to Washington, D.C. to help the government and the country think of creative ways to use information technology to improve our economy and address important social problems.

He is a patriot and the son of immigrants who have played their own role in keeping the American economy vibrant and expanding. Mr. Park's parents are here today. Mr. Park's wife is here today. Mr. Park's pastor is here today as well as friends from the IT business world. I mention this to remind all the Members to not confuse their feelings towards the Affordable Care Act with Mr. Park as a person. He served the public and did his best and should be thanked for his contributions. In fact, Mr. Park has returned to the Bay Area and is attempting to recruit other bright, innovative stars from the IT world to come to Washington and take a few years to try to make a difference for the good of the country. Good luck with that message after today, Mr. Park.

I have reviewed a Minority staff report, which I ask be made part of the record, built on a complete review of the documents produced by the White House. The staff make a very strong argument, supported by White House documents, that Park did not have deep, direct, or intimate involvement in any of the work of developing the on-line marketplace launched on October 1, 2013 or the cybersecurity standards and techniques used for the site.

If he was playing such a role, there should be monthly progress reports from contractors that show progress against deliverables and requirements, costs of work, a critical path analysis that identifies where problems threaten a successful launch and discussion of the integration process for the site across an army of contractors on the project. None of those documents have been produced because he was not the day-to-day manager on the project. Nor are there the kind of documents that the contractors doing the actual work would possess—which would include discussion of code, performance and testing results. Those documents can be found at CMS, which managed this complex acquisition, and among the contractors, who did the work, but not in Todd Park's records.

The records that did come to us make it very clear what he was doing: He acted to gather information when the White House had questions about the project and he acted to help CMS find resources when they asked for help from the White House. 90% of the records fall into one category or the other. Gathering information for the boss or to use as a spokesman or providing assistance to the actual managers sounds more like the kind of work our Legislative Assistants and Committee staff do than that of people deeply involved in a project. The record shows Park was not in charge of anything, and what he did do on healthcare.gov was about information aggregation or assistance at the request of others.

There is another missing element in the records the Committee has received from the White House: the thousands of pages of records related to Mr. Park's full time job as Chief Technology Officer of the United States. Because we only requested records related to HealthCare.gov, it is easy to lose sight of the fact that his very limited work on Healthcare.gov was coming while he did a wide-ranging job as CTO.

Park's job was about trying to push technology throughout all levels of the country to improve our competitiveness and quality of life. As just one example, he drove an initiative to find innovative methods to use IT and big data to combat human trafficking. I don't think there is any Member who favors human trafficking—that is about as non-partisan an initiative as you can get. Park was working, full time, in a much wider swath of issues and areas than healthcare.gov. Members should never lose sight of that and get tunnel vision about Park simply because we have such a narrow set of records.

I believe that if Mr. Park is given a fair chance to answer questions here today, that Members on both sides of the aisle will conclude that Park was not a principal actor in the development of HealthCare.gov prior to October 1, 2013 and had no role in developing cybersecurity standards or techniques for the web site. Mr. Park, I am going to apologize to you now for the way you have been treated, and I am hopeful that you will get apologies from the Chairman by the end of this hearing.

SUPPORTING DOCUMENTS SUBMITTED BY SUBCOMMITTEE CHAIRMAN PAUL BOURN

LAMAR S. SMITH, Texas
CHAIRMANEDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.scienc.house.gov

December 11, 2013

President Barack Obama
The White House
1600 Pennsylvania Ave., N.W.
Washington, DC 20500

Dear Mr. President:

We write to request information and an explanation about what your Administration is doing to address the security risks and privacy concerns surrounding Healthcare.gov. During a teleconference with reporters on December 1, Mr. Jeffrey Zients, your National Economic Council Director-designate, stated that the Obamacare website is “night and day from where it was on October 1” and that the website can now “support intended volumes” of users.¹

Though we appreciate the Administration’s efforts to address the flaws with the website’s capacity, we are concerned that the larger security and privacy issues remain unaddressed. While more people may be able to access the website, without much-needed security enhancements, this simply means that more Americans are vulnerable to online criminals and identity theft.

At a hearing before the House Committee on Science, Space, and Technology on November 19, leading computer security experts from the private sector and academia outlined the significant threats posed to Americans by identity theft. One witness, David Kennedy, is a so-called “white hat hacker” who helps private sector companies secure their websites and data from online criminals. Mr. Kennedy gave a demonstration of real vulnerabilities with Healthcare.gov, showing how hackers are attempting to access personal information on the website. According to his testimony, not only is the website vulnerable, it’s under active attack. Even more troubling, Mr. Kennedy testified that there are “clear indicators that even basic security was not built into the Healthcare.gov website.”

By design, Healthcare.gov interfaces with numerous federal, state and commercial sites and databases. The data passing through the Healthcare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. To gain information on

¹ CBSNEWS.COM Staff, “Healthcare.gov improvements ‘night and day’ from October launch,” CBSNEWS.COM, December 1, 2013, available at: <http://www.cbsnews.com/news/healthcaregov-improvements-night-and-day-from-october-launch/>

Mr. President
December 11, 2013
Page 2

potential healthcare coverage through the website, users must input personal contact information, birth dates and social security numbers, as well as income, tax and other intimate financial information.

Although the website itself does not retain personal data, it transmits it to other sites. Without adequate security measures, Healthcare.gov essentially becomes a portal for online criminals to access even more sensitive, personal data maintained by the IRS, state agencies, and insurance companies that share information with the website. The size and scope of information sharing alone raises significant security concerns.

When asked whether Healthcare.gov had been compromised by hackers, Mr. Kennedy testified that he believed the website already has been hacked or soon will be. Every single witness, majority and minority-invited alike, testified that Healthcare.gov is not secure. Asked if they would have launched the website, the unanimous answer was “No.” Would they require front-end personal data disclosure on the site? Again, all four responded “No.” Finally, each of the experts said taking down Healthcare.gov should be seriously considered to address the security concerns and protect the personal information of users. Mr. President, your Administration has an obligation to ensure that the personal, financial, and account information collected as part of the Affordable Care Act is secure.

Unfortunately, in its haste to launch the Healthcare.gov website, it appears that your Administration has cut corners that have left the website open to hackers and other online criminals. As a result, the personal information that has already been entered into Healthcare.gov is vulnerable to identity thieves. We already know of many attempts to hack into the system. If the security flaws go unaddressed, the more people who use the site will simply mean more Americans vulnerable to identity theft.

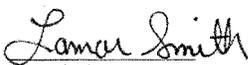
In light of the concerns of online security experts, the following questions need to be addressed to ensure the safety, security, and privacy of all Americans’ personal data on the Obamacare website.

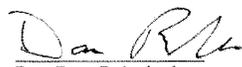
- 1) Since October 1, what explicit steps has the Administration taken to improve the security of Healthcare.gov?
- 2) Who in the Administration has been assigned to monitor, manage, and oversee the ongoing security needs of Healthcare.gov?
- 3) Has the Administration conducted thorough, on-going tests and monitoring of security and privacy vulnerabilities with Healthcare.gov—including hiring private sector “hackers” to test the website’s ability to guard against malicious attack and intrusion? If so, who conducted the tests and on what dates? What were the operational details and specific results of these security tests?

Mr. President
December 11, 2013
Page 3

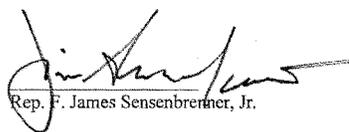
Because of the seriousness of the threat facing users of Healthcare.gov, we ask that answers to these critical questions be provided to the Committee no later than December 18.

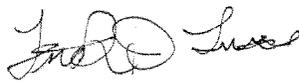
Sincerely,

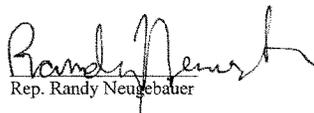

Lamar Smith
Chairman

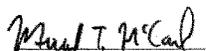

Rep. Dana Rohrabacher

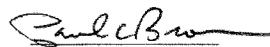

Rep. Ralph M. Hall

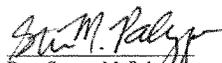

Rep. F. James Sensenbrenner, Jr.

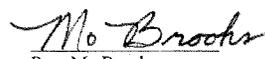

Rep. Frank D. Lucas


Rep. Randy Neugebauer

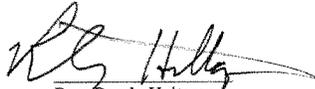

Rep. Michael T. McCaul

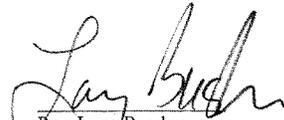

Rep. Paul C. Broun

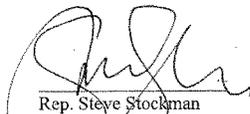

Rep. Steven M. Palazzo


Rep. Mo Brooks

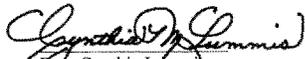
Mr. President
December 11, 2013
Page 4

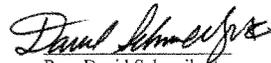

Rep. Randy Hultgren

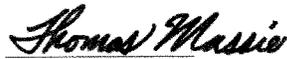

Rep. Larry Bucshon

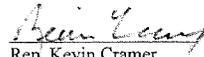

Rep. Steve Stockman


Rep. Bill Posey

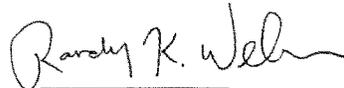

Rep. Cynthia Lummis


Rep. David Schweikert

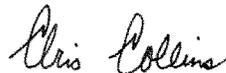

Rep. Thomas Massie


Rep. Kevin Cramer


Rep. Jim Bridenstine


Rep. Randy Weber


Rep. Chris Stewart


Rep. Chris Collins

Mr. President
December 11, 2013
Page 5

cc: Rep. Eddie Bernice Johnson
Ranking Member

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

January 15, 2014

The Honorable Lamar S. Smith
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith,

I write in response to your letters of December 11 and 20, 2013, which discuss the Committee's "efforts to examine the safety, security and privacy of Americans' personal data through the Obamacare website."¹ At the outset, thank you for your recognition that the performance of the healthcare.gov website has improved, though you continue to express concerns about the security and privacy of the technological infrastructure that allows Americans to shop for and purchase high-quality, affordable health insurance.

Your most recent letters are two in a series that discuss the Committee's oversight interest in the security of the Federal healthcare exchange. As the Office of Science and Technology Policy (OSTP) has repeatedly explained, OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace's (FFM) security measures. Nevertheless, OSTP has tried to address the Committee's interest, including offering to testify regarding cybersecurity issues generally, and we remain committed to working with the Committee on science and technology matters.

Portions of your December 20 letter, however, indicate that you may continue to misunderstand which agency is responsible for the security of the FFM. As you know from our prior correspondence, primary responsibility for monitoring, managing, and overseeing the security of the FFM rests with the Centers for Medicare and Medicaid Services (CMS). Congress has received a wealth of information from CMS regarding the security of the FFM in both testimony and written responses, and I trust you have access to this information.² CMS and the Department

¹ December 20 Letter at 3.

² *See, e.g.*, July 17, 2013 – CMS Administrator Tavenner's Testimony before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies and House Oversight and Government Reform Subcommittee on Energy Policy, Health Care and Entitlements, Joint Hearing on Information Sharing and the 2010 Health Care Overhaul Law; Aug. 1, 2013 – CMS Administrator Tavenner's Testimony before the House Energy and Commerce Committee, Hearing on Implementation of the 2010 Health Care Overhaul Law; Sept. 11, 2013 – HHS Assistant Inspector General for Audit Services Kay Daly's Testimony before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, Hearing

of Health and Human Services (HHS) have explained that the privacy and security of consumers' personal information is a top priority; that when consumers fill out their online Marketplace applications, they can trust that the information that they provide is protected by stringent security standards; and that, to date, there have been no successful security attacks on healthcare.gov and no person or group has maliciously accessed personally identifiable information from the site.³

Your most recent letter states that you seek information on the security and privacy of the FFM from U.S. Chief Technology Officer (CTO) Todd Park based on "his familiarity with the website while he was CTO for the US Department of Health and Human Services."⁴ It is true that Mr. Park helped develop the initial version of healthcare.gov when he worked for HHS in 2010. But the first iteration of healthcare.gov on which Mr. Park worked served as a general source of information about the Affordable Care Act, healthcare insurance options, hospital quality, and prevention topics. It was not a transactional marketplace on which consumers could purchase healthcare insurance, and it bears little resemblance to the current version of the website. That first version of the website has been replaced by the current healthcare.gov website, which is the interface for the FFM, and—as is well known—was developed by Federal contractors under CMS' supervision. As OSTP has explained, CMS is best positioned to discuss the security of the FFM.

Your letter also seeks information from Mr. Park about the security of healthcare.gov based on his role, as one of three co-chairs, in the Interagency Steering Committee. The Steering Committee focused on interagency coordination of the healthcare exchange and, in particular, the "data services hub" that facilitates communication among Federal and State agencies in connection with the purchase of health insurance by customers. As even the document attached to your December 20 letter makes clear, the agencies actually developing the hub, particularly CMS, IRS, and SSA, were assigned lead responsibility for working on data privacy and security harmonization issues that required interagency coordination. Making these agencies responsible for the security of the FFM made practical sense and was consistent with the applicable legal framework: that is, each Federal department and agency retains primary responsibility for securing and defining its own networks and critical information infrastructure.⁵ As OSTP has explained before, OSTP personnel have not been substantially involved in developing or implementing the security measures in place to protect the FFM.

on the Health Exchange Data Hub; Oct. 30, 2013 – HHS Secretary Sebelius' Testimony before the House Energy and Commerce Committee, Hearing on the 2010 Health Care Law Enrollment Issues; Oct. 29, 2013 – CMS Administrator Tavenner's Testimony before the House Ways and Means Committee, Hearing on the 2010 Health Care Law Enrollment Challenges; Dec. 11, 2013 – HHS Secretary Sebelius' Testimony before the House Energy and Commerce Subcommittee on Health, Hearing on the Implementation of the 2010 Health Care Law.

³ See House Energy and Commerce Minority Memo of December 13, 2013, summarizing HHS briefing, <http://democrats.energycommerce.house.gov/sites/default/files/documents/Memo-ACA-Security-Briefing-2013-12-13.pdf>; see also Healthcare.gov Privacy Policy, <https://www.healthcare.gov/privacy/>.

⁴ December 20 Letter at 2.

⁵ See, e.g., Nov. 13, 2013 - Department of Homeland Security Acting Assistant Secretary Stempfley's Testimony before the House Homeland Security Committee, Hearing on Data Security as it Relates to the Federal Government Website, HealthCare.gov, and the 2010 Health Care Law.

Nevertheless, in a further effort to accommodate the Committee's interest in this area and to help clarify the role of OSTP personnel, we are providing with this letter documents regarding certain interagency meetings, mainly the meetings of the Interagency Steering Committee, including agendas and associated materials that make reference to security. (Staff on Chairman Issa's committee appear to have given some of these materials to you already, but we are producing them here at your request and for your convenience.) Nothing in the enclosed documents indicates that Mr. Park had a substantial role in developing or managing the security aspects of the FFM; they only serve to confirm that a briefing from Mr. Park on those issues would be neither informative nor productive.

Finally, your letter states that the Administration has rejected three invitations to testify before the Committee and incorrectly asserts that OSTP raised Executive Privilege concerns in response to these invitations. To the contrary, OSTP has repeatedly made efforts to address the Committee's stated oversight interest in the safety and security of the FFM. On at least four occasions, OSTP has offered to provide one of its two Senate-confirmed leaders, OSTP Associate Director for National Security and International Affairs Patricia Falcone, to testify. Dr. Falcone does not have specific knowledge of the data-security standards in place for healthcare.gov, but she is knowledgeable about general cybersecurity policy issues, including a cybersecurity report that your staff identified as relevant to its inquiry when first seeking an OSTP witness to testify before the Committee.⁶ To my knowledge, OSTP has not mentioned or relied on a claim of Executive Privilege. Reviewing OSTP's prior correspondence with you and your staff, I see no mention of it, and Dr. Holdren does not recall referring to it in his conversation with you. The Committee has not addressed the previous offers that we have made, but OSTP has been—and continues to be—willing to accommodate the Committee's oversight interest by having Dr. Falcone testify on general cybersecurity policy issues.

I trust you will find the additional information we provide with this letter helpful. OSTP will be addressing the questions posed in your December 20 letter regarding the Presidential Innovation Fellows program under separate cover. In the meantime, OSTP looks forward to continuing to work with you on science and technology issues.

Sincerely,



Donna M. Pignatelli
Legislative Affairs Director

⁶ Email from H. Comm. on Science, Space, & Technology Majority Staff to OSTP staff (Oct. 28, 2013, 5:42 p.m.) ("I suspect we would touch on related issues raised and addressed in the 'Cyberspace Policy Review' and the Dec 2011 report 'Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,' both of which were referred to in Dr. Holdren's testimony before the Committee in a full committee oversight hearing on June 20, 2012.")

cc: The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space and Technology

Enclosure

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

January 15, 2014

The Honorable Lamar S. Smith
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith,

Thank you for your letter of December 20, 2013, in which you requested information about the Presidential Innovation Fellows (PIF) program. The PIF program pairs top innovators from the private sector, non-profits, and academia with top innovators in government to collaborate during focused 6-12 month "tours of duty" to develop solutions that can save lives, save taxpayer dollars, and fuel job creation.

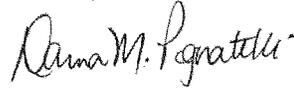
The first round of five projects was launched in August 2012 with 18 inaugural Fellows. For that first round of Fellows in 2012, OSTP worked with agencies to identify potential projects, launched the PIF program and solicited applications, and forwarded all applications to participating Federal agencies. Federal agencies then conducted reviews and interviews of the applicants, identified relevant skills and expertise, and directly hired Fellows to work on projects aimed at supporting entrepreneurs, small businesses, and the economy.

For the second round of PIFs, OSTP gradually transitioned the program to GSA's management. The two agencies jointly coordinated the application process, and GSA managed the hiring process, selected the PIFs with significant input from the agencies sponsoring the PIF projects, and assigned Fellows to agencies as detailees on a cost-recoverable basis. Going forward, GSA is expected to administer the PIF hiring process.

You also asked specifically about PIFs at The Center for Medicare and Medicaid Services (CMS). As part of the "tech surge" announced in October 2013, CMS brought in top experts from both inside and outside government to help improve healthcare.gov. This "tech surge" includes two PIFs employed by GSA and detailed to CMS under fully-reimbursable detail agreements. The Fellows were selected on the basis of specific technical skills that had been identified by the healthcare.gov team as high priority needs, including large scale platform development and identity management. The two Fellows working at CMS are scheduled to complete their details in approximately one month, on February 14, 2014.

OSTP looks forward to continuing to work with you on science and technology issues.

Sincerely,

A handwritten signature in black ink that reads "Donna M. Pignatelli". The signature is written in a cursive style with a horizontal line underlining the name.

Donna M. Pignatelli
Legislative Affairs Director

cc: The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space and Technology

LAMAR S. SMITH, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

December 20, 2013

The Honorable John P. Holdren
Assistant to the President for Science and Technology
Director, Office of Science and Technology Policy
The White House
Washington, DC 20502

Dear Dr. Holdren:

At a hearing held on November 19, the Committee on Science, Space, and Technology received troubling testimony¹ from online security experts regarding the flaws and vulnerabilities in the Obamacare website that put the personal data of Americans at risk. The expert witnesses at our hearing outlined the significant risk of identity theft to Americans if hackers gained access to their personal information. One of the witnesses, Mr. David Kennedy, is a ‘white hat hacker’ who gave a demonstration of real vulnerabilities with Healthcare.gov, showing how hackers are attempting to access personal information on the website. According to his testimony, not only is the website vulnerable, it is under active attack. Even more troubling, Mr. Kennedy testified that there are “clear indicators that even basic security was not built into the Healthcare.gov website.”²

The Administration’s recent efforts to address the flaws with the website’s capacity do not appear to address the larger security and privacy issues raised in our hearing. According to Mr. Jeffrey Zients, who is in charge of fixing the website, the Obamacare website is “night and day from where it was on October 1,”³ and it is now “stable and operating at intended capacity with greatly improved performance.”⁴ Unfortunately, the improved performance does not include much-needed security enhancements, meaning that more Americans could now be vulnerable to online criminals and identity theft. According to a blog post by Mr. Kennedy, “Out

¹ House Committee on Science, Space and Technology hearing, “*Is My Data on Healthcare.gov Secure?*” November 19, 2013, available at: <http://science.house.gov/hearing/full-committee-hearing-my-data-healthcaregov-secure>.

² Testimony of Mr. David Kennedy, CEO, TrustedSec, at House Committee on Science, Space and Technology hearing, “*Is My Data on Healthcare.gov Secure?*” November 19, 2013 available at: <http://science.house.gov/hearing/full-committee-hearing-my-data-healthcaregov-secure>.

³ CBSNEWS.COM Staff, “HealthCare.gov improvements ‘night and day’ from October Launch,” CBSNEWS.COM, December 1, 2013, available at: <http://www.cbsnews.com/news/healthcaregov-improvements-night-and-day-from-october-launch>.

⁴ *Ibid.*

Dr. Holdren
December 20, 2013
Page 2

of all of the reports, there were no mention to security concerns or addressing the vulnerabilities identified in the healthcare.gov website...a number of undisclosed exposures have still not been addressed and exist today.”⁵

Through its jurisdiction over the White House Office of Science and Technology Policy (OSTP), the Committee sought to hear from Mr. Todd Park, OSTP’s Chief Technology Officer (CTO), given his familiarity with the website while he was CTO at the US Department of Health and Human Services (HHS). As you yourself stated upon his hire to OSTP, while at HHS, Mr. Park “led the successful execution of an array of breakthrough initiatives, including the creation of HealthCare.gov.”⁶

Additionally, according to the OSTP website, the Administration and OSTP are committed to advancing policies that will “safeguard the privacy of every American by strengthening digital security systems and holding governments and businesses accountable for violations of personal privacy.”⁷

Notwithstanding Mr. Park’s background and leadership position within OSTP, the Administration has now rejected three invitations to Mr. Park to testify before the Committee. You stated in a recent phone conversation with Chairman Smith that Mr. Park’s testimony would raise claims of Executive Privilege – despite the fact that Mr. Park already testified before a congressional committee on November 13.⁸ Your staff has similarly suggested that Mr. Park’s activities are protected by Executive Privilege, begging the question: does the Administration intend to invoke such a claim?

You also stated in your November 26 letter to Chairman Smith that Mr. Park has not been involved in the security issues of the Healthcare.gov website. That assertion appears to be contradicted by the fact that Mr. Park was one of three White House co-chairs of the Affordable Care Act (ACA) Information Technology Exchanges Steering Committee (see Attachment 1).

The stated mission of this Healthcare.gov Steering Committee is to support the timely and efficient resolution of barriers to assure the implementation of “consumer-centric” health insurance exchanges. The Steering Committee’s Charter explicitly directs the participants “to promote resolution of key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government and with the state exchanges,” and to “direct the formulation of work groups to identify barriers, develop and identify promising practices to support efficiencies, and develop option papers for the Committee’s consideration.” (Attachment

⁵ David Kennedy, “Healthcare.gov Operational – Security concerns not addressed,” TrustedSec, December 2, 2013, available at: <https://www.trustedsec.com/december-2013/healthcare-gov-operational-security-concerns-not-addressed>.

⁶ John Holdren, “Todd Park Named New U.S. Chief Technology Officer,” The White House Blog, March 9, 2012, available at: <http://www.whitehouse.gov/blog/2012/03/09/todd-park-named-new-us-chief-technology-officer>.

⁷ OSTP website, “Technology and Innovation,” available at: <http://www.whitehouse.gov/administration/eop/ostp/divisions/technology>

⁸ House Committee on Oversight and Government Reform, “ObamaCare Implementation: The Rollout of HealthCare.gov,” November 13, 2013, available at: <http://oversight.house.gov/hearing/obamacare-implementation-rollout-healthcare-gov/>.

Dr. Holdren
December 20, 2013
Page 3

1). The ACA Exchanges Steering Committee directly oversees both security and privacy interagency working groups (Attachment 1).

From documents provided to Congress, it also appears that this White House-led Steering Committee canceled several meetings scheduled over the course of the past year following an April briefing on a White House-requested report by McKinsey & Company that warned of “various problems with the exchange, including limited testing time and resources before the launch.”⁹ After repeatedly cancelling Steering Committee meetings for five consecutive months, the White House Steering Committee met again only weeks prior to the launch of the Healthcare.gov website on October 1. But as we now know, those actions were too little and too late.

It is logical to assume that security and privacy responsibility resides at the highest level of government. The data passing through the Healthcare.gov website is one of the largest collections of personal information ever assembled, linking social security numbers, birth dates, tax and other financial information from seven different federal agencies, along with state agencies and government contractors. We are troubled by the fact that the President either did not know, or did not care, that the personal and financial data collected as part of Obamacare is not secure.

The Committee will continue its efforts to examine the safety, security and privacy of Americans’ personal data through the Obamacare website. Part of those efforts includes oversight of OSTP’s role in the Healthcare.gov website. To that end, please provide the following documents from your agency by January 3, 2014:

- (1) All schedules and scheduling information (as defined in Attachment 2) for Mr. Todd Park since arriving at OSTP through the present on topics involving the Healthcare.gov website and related issues.
- (2) All records and emails (as defined in Attachment 2) to or from any and all OSTP employees, including Mr. Todd Park, regarding the ACA, Healthcare.gov, or the ACA Information Technology Exchanges Steering Committee.
- (3) All records and information regarding any and all briefings (as defined in Attachment 2) with the President and/or White House staff on Healthcare.gov and related issues.
- (4) Copies of all records provided in the past, as well as those expected to be provided in the future, by OSTP to other congressional committees in response to any ACA or Healthcare.gov document requests.

In responding to the Committee’s request, please provide a Vaughn Index for any redactions or documents withheld from us. Specifically, for each redaction and document withheld on the basis of an established and accepted privilege, please provide a log containing the following information:

⁹ Jim Acosta and Dana Davidsen, “Private consulting firm warned of glitches before healthcare.gov launch,” CNN Politics, November 19, 2013, available at: <http://politicalticker.blogs.cnn.com/2013/11/19/private-consulting-firm-warned-of-glitches-before-healthcare-gov-launch>.

Dr. Holdren
December 20, 2013
Page 4

- (1) the privilege asserted;
- (2) the type of document;
- (3) the general subject matter;
- (4) the date, author, and addressee, and
- (5) the relationship of the author and the addressee to each other.

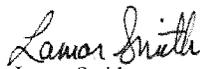
In addition to these documents, please also provide responses to the following questions by January 3, 2014:

- 1) As previously mentioned, in your phone conversation with Chairman Smith, you stated that Mr. Park's testimony would raise claims of Executive Privilege. Please confirm this assertion, and if you intend to invoke such a claim, please clarify whether you are basing it on Mr. Park's position as CTO at OSTP, or as Assistant to the President?
- 2) Please explain Mr. Park's relationship relative to the Presidential Innovation Fellows program. Please also provide details about which Fellows have been tapped to work on the Healthcare.gov website as part of the 'tech surge' to fix its problems. Your response to this question should include the names of the Fellows, who selected them to work on the website, when they started work on the website, whether they are still working on it and how much longer they are expected to work on it.
- 3) Finally, please direct Mr. Park to make himself available to Committee staff for a briefing on his involvement with the website prior to and subsequent to the October 1st launch date. Please ensure that this meeting takes place before January 10, 2014.

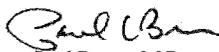
In its haste to launch the Healthcare.gov website, it appears the Obama Administration cut corners that leave the site open to hackers and other online criminals. As a result, Americans who have already entered personal information into Healthcare.gov are vulnerable to identity theft. We already know of numerous attempts to hack into the system and can only assume many more have gone unreported. Unless the Obama Administration takes swift action to address security, it is likely the worst is yet to come.

If you have any questions, please have your staff contact Raj Bharwani, Subcommittee on Oversight Staff Director, at (202) 225-6371.

Sincerely,



Lamar Smith
Chairman
Committee on Science, Space,
and Technology



Paul Broun, M.D.
Chairman
Subcommittee on
Oversight



Larry Bucshon, M.D.
Chairman
Subcommittee on
Research & Technology

Dr. Holdren
December 20, 2013
Page 5

cc: Rep. Eddie Bernice Johnson
Ranking Member
Committee on Science, Space,
and Technology

Rep. Dan Maffei
Ranking Member
Subcommittee on Oversight

Rep. Dan Lipinski
Ranking Member
Subcommittee on Research & Technology

Attachments



**Affordable Care Act IT Exchanges
Steering Committee
Charter**

May 21, 2012

Project: Interagency Coordination for ACA IT Exchanges

TABLE OF CONTENTS

I. PURPOSE	2
II. MISSION	2
III. SCOPE AND RESPONSIBILITIES	2
IV. MEMBERSHIP AND REPORTING STRUCTURE	4
V. ADMINISTRATION	5
VI. AGREEMENT	6

I. Purpose

This charter establishes the Affordable Care Act (ACA) IT Exchanges Steering Committee (Steering Committee) as a collaborative body and as a venue for seeking resolution of persistent interagency challenges and dependencies related to the implementation of IT exchanges in support of the Affordable Care Act.

This document outlines the mission, scope and responsibilities of the Steering Committee, identifies membership and support structures, and defines key processes and procedures. A Health Exchange Executive Secretariat (Executive Secretariat) has been established as an agent of the Committee to work with Agencies to ensure projects fully align under the Affordable Care Act in providing a streamlined and seamless interface with the American public and affected industries that will be impacted by the implementation of the health insurance exchanged under the Affordable Care Act.

II. Mission

The primary mission of the Steering Committee is to support the timely and efficient resolution of barriers while ensuring the realization of fully operational health insurance exchanges mandated under the Affordable Care Act. The Steering Committee will (a) address key Exchange information sharing policies and barriers; (b) work with Departments, Agencies, and other stakeholders as necessary on the implementation and execution of Health Insurance Exchanges.

III. Scope and Responsibilities

Steering Committee

The Steering Committee shall provide a forum for seeking resolution of interagency challenges and to further promote interagency alignments to assure the implementation of a consumer-centric health insurance exchanges under the Affordable Care Act. The Steering Committee can designate the Executive Secretariat to act on its behalf to meet these functions. The Steering Committee shall:

- Facilitate interagency discussions to promote resolution to key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government and with the state exchanges
- Direct the formulation of work groups to identify barriers, develop or identify promising practices to support efficiencies, and develop option papers for the Committee's consideration.

- The Steering Committee will meet monthly or more frequently as deemed necessary by the Executive Secretariat, beginning in May 2012 through March 2014. The meeting frequency may be altered by the agreement of the Steering Committee Co-Chairs. Beginning in April 2014, the Steering Committee will meet on an *ad hoc* basis as advised by the Executive Secretariat or as requested by the Co-Chairs until it is the consensus of the Steering Committee members that the Exchange post-implementation issues have been sufficiently surfaced and addressed.

Executive Secretariat

The Executive Secretariat reports to the co-chairs and will support, coordinate, and act as a liaison between the Steering Committee and Departments.

The Executive Secretariat will remain operational through January 2015 or until it is the consensus of the Steering Committee members that the Exchange post-implementation issues have been sufficiently surfaced and addressed.

- Lead: HHS Program Management Office, Office of the Chief Information Officer
- Members: CMS, IRS, SSA

The Executive Secretariat's core functions will be as follows:

- Work with the designated workgroups to identify interagency IT policy issues for the Steering Committee's consideration.
- Responsible for tracking and reporting progress of individual workgroups and elevating workgroup concerns to the Steering Committee.
- Share recommendation from the Steering Committee with workgroups and Agencies; distribute and support the implementation of these recommendations.
- Work closely with Agencies and stakeholders to develop and iterate the plans for resolution of challenges as appropriate.

Agencies will continue to coordinate ACA IT exchange project governance and oversight functions within their respective organizations and work directly with their IT project teams to ensure performance and alignment with the Steering Committee recommendations as appropriate.

Working Groups

Data Sharing and Privacy

- **Objectives:** Streamlining data use agreements and creating a uniform process for developing and maintaining computer matching agreements, data use agreements, ICAs, consent forms, etc..
- **Lead:** Janet Miner, IRS
- **Members:** HHS, SSA, DHS, VA, OPM, DoD, Peace Corps.

Security Harmonization

- **Objectives:** Coordinate uniform process to harmonize security and streamline negotiations/documentation of new agreements within and across each agency
- **Co-Leads:** Tim May, SSA & Tom Schankweiler, CMS
- **Members:** HHS, IRS, VA, DHS, Peace Corps, OPM

Operational Oversight

- **Objective:** Provide a clearinghouse for issues needing to be analyzed and resolved among agencies for those issues not covered by other more specific workgroups, issue tracking and execution of common priorities in a timely/effective manner, and to assure the maximal alignment with the vision for a consumer-centric insurance exchange
- **Co-Leads:** Jim Kerr, CMS, Wanda Brown (IRS)
- **Members:** HHS, IRS, SSA, VA, DHS, Peace Corps, DoD, OPM

IV. Membership and Reporting Structure

The Federal Chief Information Officer (CIO), the Health Program Associate Director, and the U.S. Chief Technology Officer (CTO), in the Executive Office of the President will serve as co-Chairpersons for the Affordable Care Act IT Steering Committee. Membership will be comprised of senior executives from each of the participating Departments and Agencies who understand the ACA and health insurance exchange-related IT and business/mission needs of their Departments and Agencies and who can make key policy and management judgments on behalf of the respective Departments.

The following Departments and Agencies are represented on the Committee and will designate a senior executive as described above as members of the Steering Committee:

- Department of Health & Human Services, Centers for Medicare and Medicaid Services
- Department of Treasury, Internal Revenue Service
- Department of Homeland Security
- Department of Defense
- Department of Veterans Affairs

- Social Security Administration
- Peace Corps

Additional members may be added if additional interagency dependencies are identified.

Representatives from other Departments and offices, including subject matter experts (SMEs) and other advisors, may be invited to attend Steering Committee meetings with the concurrence of the Steering Committee co-Chairs.

V. Administration

A. Meetings

The Steering Committee shall meet as needed and as advised by the Executive Secretariat. Meetings may be in person, by conference call, or other "virtual" meeting tools. Materials shall be distributed to the members prior to the meeting in order for the members to have adequate time to review and consider the material. The members will be requested to review and provide comment/feedback on materials as appropriate.

B. Records Management

The Executive Secretariat will be responsible for appointing a designee to distribute materials prior to and post meetings (i.e., agenda, meeting minutes).

ATTACHMENT

1. The term "records" is to be construed in the broadest sense and shall mean any written or graphic material, however produced or reproduced, of any kind or description, consisting of the original and any non-identical copy (whether different from the original because of notes made on or attached to such copy or otherwise) and drafts and both sides thereof, whether printed or recorded electronically or magnetically or stored in any type of data bank, including, but not limited to, the following: correspondence, memoranda, records, summaries of personal conversations or interviews, minutes or records of meetings or conferences, opinions or reports of consultants, projections, statistical statements, drafts, contracts, agreements, purchase orders, invoices, confirmations, telegraphs, telexes, agendas, books, notes, pamphlets, periodicals, reports, studies, evaluations, opinions, logs, diaries, desk calendars, appointment books, tape recordings, video recordings, e-mails, voice mails, computer tapes, or other computer stored matter, magnetic tapes, microfilm, microfiche, punch cards, all other records kept by electronic, photographic, or mechanical means, charts, photographs, notebooks, drawings, plans, inter-office communications, intra-office and intra-departmental communications, transcripts, checks and canceled checks, bank statements, ledgers, books, records or statements of accounts, and papers and things similar to any of the foregoing, however denominated.
2. The terms "relating," "relate," or "regarding" as to any given subject means anything that constitutes, contains, embodies, identifies, deals with, or is in any manner whatsoever pertinent to that subject, including but not limited to records concerning the preparation of other records.

LAMAR S. SMITH, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

March 27, 2014

The Honorable John P. Holdren
Director
Office of Science and Technology Policy
Executive Office of the President
725 17th Street NW, Room 5228
Washington, DC 20502

Dear Dr. Holdren,

Thank you for testifying before the Committee on Science, Space, and Technology yesterday. As discussed, there are differences in budget priorities where we will simply have to agree to disagree. While we have differences of opinion, there is no reason to have differences in facts. I am concerned that you created some confusion in your explanation for why Chief Technology Officer Todd Park refuses to testify before the Committee about his role in Healthcare.gov.

Yesterday, you claimed that Mr. Park "doesn't report to me...I can't compel him to come and testify." The statement that he doesn't report to you appears to contradict your November 26 letter to me that stated, "Mr. Park is part of OSTP's leadership". On the OSTP website, Mr. Park is listed as a member of your leadership team and that he is in charge of a 14-staff division within your Office. Further, you wrote a blog post on March 9, 2012, to welcome Mr. Park to OSTP and explained his duties. If Mr. Park doesn't report to you, to whom does he report?

Likewise, you repeated the statement that Mr. Park "has not been primarily associated with the security of the [Healthcare.gov] site." Mr. Park was the Chief Technology Officer at the Department of Health and Human Services from August 2009 until March 2012, where he led development of Healthcare.gov prototype before joining OSTP. After that, Mr. Park was a White House Co-Chairman of the Affordable Care Act Information Technology Exchanges Steering Committee that even had an interagency Healthcare.gov security subcommittee directly reporting to him. The only way the Science, Space, and Technology Committee learned about Mr. Park's role was through media reports, and never directly from your office.

Would you correct or clarify your testimony on this important subject? Further, I hope that you will change your position about not allowing Mr. Park to testify.

Sincerely,



Lamar Smith
Chairman

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

November 14, 2013

The Honorable Lamar S. Smith
Chairman
House Committee on Science, Space, and Technology
2321 Rayburn HOB
Washington, D.C. 20515

Dear Chairman Smith,

Thank you for your letter of November 13, 2013, inviting Todd Park to testify at a December 5, 2013, hearing before the Committee on Science, Space, and Technology that will address the security standards and technical measures to protect personal information on the healthcare.gov website.

As I explained previously in my November 8th letter to the Committee, the Office of Science and Technology Policy (OSTP) has not been substantially involved in the privacy and security standards for healthcare.gov. Thus, neither Mr. Park nor any other OSTP staff member is in a position to testify on the data security standards of the website.

Indeed, when asked about the security features of the healthcare.gov website during a hearing yesterday before another committee, Mr. Park explained that he has not been working on these issues and suggested that the Centers for Medicare and Medicaid Services (CMS) security team is better situated to answer such questions. As I have offered previously, however, I remain willing to check the availability of OSTP Associate Director for National Security and International Affairs Patricia Falcone to testify on general cybersecurity issues, as she has worked on cybersecurity policy since her confirmation. But if the focus of the hearing will be the data security standards for healthcare.gov, OSTP must defer to CMS, which is better positioned to accurately answer any questions.

Finally, as you know, longstanding OSTP policy ordinarily permits only Senate-confirmed staff to testify before Congress. Our current staff consists of two Senate-confirmed individuals: Dr. John Holdren, our Director, and Dr. Falcone. If you wish, I am available to continue discussions with your staff regarding Dr. Falcone or an alternative witness for the hearing. In this event, OSTP requests that the hearing take place the week of December 9-13 or later, given scheduling conflicts the first week of December.

109

I appreciate your letter and look forward to continuing to work with you and the Committee on science and technology issues.

Sincerely,

A handwritten signature in black ink that reads "Donna M. Pignatelli". The signature is written in a cursive style with a large initial 'D'.

Donna M. Pignatelli
Assistant Director for Legislative Affairs

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.sciencetechnology.house.gov

November 18, 2013

The Honorable John P. Holdren
Director, Office of Science and Technology Policy
Executive Office of the President
725 17th Street NW, Room 5228
Washington, DC 20502

Dear Dr. Holdren,

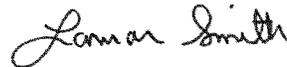
The Science, Space, and Technology Committee invited a member of OSTP leadership, Todd Park, to testify before the Committee on December 5th on the role of OSTP in setting internet policies related to the healthcare.gov website, especially those related to privacy and security standards. Mr. Park has been identified as being involved in the development of the website and the so-called tech surge to fix it.

Late last Thursday, the Committee received a letter from OSTP staff that Mr. Park would not accept my invitation to testify on December 5th. While Mr. Park is not Senate-confirmed, he is identified as the only other member of OSTP leadership other than yourself on OSTP's website. Please note that on October 31st, I invited Mr. Park to testify for our hearing on November 19th. Your staff indicated a willingness to investigate his availability after November 30th before sending the letter to decline my invitation.

I am sure you agree that accountability and transparency are bedrock fundamentals for a healthy democracy, so I hope you will encourage Mr. Park to testify. Thank you for considering this request.

I am happy to discuss this issue further at your convenience.

Sincerely,



Lamar Smith
Chairman

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

November 8, 2013

The Honorable Lamar S. Smith
Chairman
House Committee on Science, Space, and Technology
2321 Rayburn HOB
Washington, D.C. 20515

Dear Chairman Smith,

Thank you for your letter of October 31, inviting Todd Park to testify before your committee on November 19 at a hearing titled, "Is Your Data on the Healthcare.gov Website Secure?"

In communications with your staff on October 30 and 31, I explained that OSTP has not been substantially involved in the privacy and security standards that are in place for healthcare.gov. The Centers for Medicare and Medicaid Services (CMS) is in a far better position to discuss the standards that are in place for the website.

I offered that, while OSTP has no one to testify on the data security standards of healthcare.gov, I would be willing to check the availability of OSTP Associate Director for National Security and International Affairs Patricia Falcone to testify on general cybersecurity issues. Dr. Falcone has worked on cybersecurity policy since her confirmation.

I explained to your staff that Mr. Park is currently working full-time to assist CMS in the ongoing and critically important efforts to quickly improve the operation of the healthcare.gov website for the millions of Americans who are seeking quality, affordable health insurance options. He cannot be pulled away from those efforts at this time.

Finally, longstanding OSTP policy ordinarily permits only Senate-confirmed staff to testify before Congress. Our current staff consists of two Senate-confirmed individuals: Dr. John Holdren, our Director, and Dr. Falcone. As you know, Mr. Park is not Senate-confirmed. If you wish, I am available to continue discussions with your staff regarding Dr. Falcone or an alternative witness for the November 19 hearing.

We appreciate your invitation and look forward to continuing to work with you and the Committee on science and technology issues.

Sincerely,

A handwritten signature in black ink that reads "Donna M. Pignatelli". The signature is written in a cursive style with a large initial 'D'.

Donna M. Pignatelli
Assistant Director for Legislative Affairs

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

April 3, 2014

The Honorable Lamar S. Smith
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith:

Thank you for the opportunity to testify before the Committee on Science, Space, and Technology on March 26 regarding the Fiscal Year 2015 budget.

In response to your letter of March 27, I believe that my hearing testimony regarding Todd Park was clear, but I am pleased to repeat here the points that I made, and that I and my office have made previously, to ensure that there is no confusion on your part or on the part of other Members.

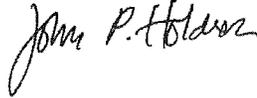
In previous correspondence, OSTP explained that Mr. Park is part of OSTP's leadership. The Office of the United States Chief Technology Officer is located in OSTP as a matter of both administrative convenience and of coordination and mutual support on substance. Inasmuch as Mr. Park's office and staff are part of OSTP—and inasmuch as he is an Assistant to the President and therefore holds the same rank as I do—it is only natural that I would consider him to be part of the OSTP leadership team, as a partner and not a subordinate. That, of course, is fully consistent with my testimony at last week's hearing.

At that hearing, I made reference to OSTP's previous statement that Mr. Park has not been primarily associated with the security of healthcare.gov. For substantiation on that point, I would refer you to a January 15, 2014, letter to you in which my office stated: "[P]rimary responsibility for monitoring, managing, and overseeing the security of the FFM rests with the Centers for Medicare and Medicaid Services (CMS)." I would further refer you to paragraphs four and five of that letter for an explanation of the points you raise in your March 27 letter.

OSTP has explained that it would not be productive for the Committee to hear from Mr. Park on the development and management of the security aspects of healthcare.gov. But we have made repeated efforts to accommodate the Committee's stated interest in the security of the site, including offering to make available OSTP's Senate-confirmed official most knowledgeable about general cybersecurity issues. We made those efforts at accommodation in no small part

because we value our relationship with the Committee. The Committee has not responded to these offers, but we remain willing to engage with the Committee on that accommodation, and on science and technology issues generally.

Sincerely,

A handwritten signature in black ink that reads "John P. Holdren". The signature is written in a cursive, flowing style.

John P. Holdren
Assistant to the President for Science and Technology
Director, Office of Science and Technology Policy

cc: The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space and Technology

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

November 13, 2013

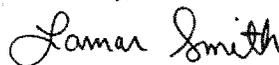
Mr. Todd Park
Chief Technology Officer
Office of Science and Technology Policy
725 17th Street, N.W.
Washington, DC 20502

Dear Mr. Park:

On October 31, 2013, I invited you to participate in a hearing to be held on November 19, 2013, before the Committee on Science, Space, and Technology (attached). Through a member of your staff, you declined to participate in the month of November due to constraints on your time with the healthcare.gov website. The Committee is inviting you to testify at a hearing on December 5, 2013, at 9:00am. The hearing will focus on the questions presented to you in the October 31, 2013, letter.

Please confirm your attendance by responding to this letter by November 15, 2013. If you have any questions, please contact Mr. Raj Bharwani, Committee on Science, Space, and Technology, at (202) 225-6371. I look forward to your participation in the hearing.

Sincerely,



Lamar Smith
Chairman

cc: Rep. Eddie Bernice Johnson
Ranking Member

Attachment

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

October 31, 2013

Mr. Todd Park
Chief Technology Officer
Office of Science and Technology Policy
725 17th Street, N.W.
Washington, DC 20502

Dear Mr. Park:

On Tuesday November 19, 2013, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building, the Committee on Science, Space, and Technology will hold a hearing titled, "Is Your Data on the Healthcare.gov Website Secure?" I am writing to formally invite you to testify at this hearing.

The hearing will examine concerns about the lack of privacy standards for personal information passing through the Healthcare.gov website and the threat posed to Americans if hackers on the Internet gained access to such information.

The data passing through the Healthcare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. In order to gain information on potential healthcare coverage through the website, users must input personal contact information, birth dates and social security numbers for all family members, as well as household salary and debt information. Users may also be asked to verify home mortgage and credit card information, place of employment, previous addresses, and whether the person has any physical or mental disabilities.

In your testimony, please be prepared to discuss what specific security standards and technical measures are in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or leaked.

You are requested to submit a written statement, which may be of any reasonable length and may contain supplemental materials; however, please be aware that the Committee cannot guarantee that supplemental material will be included in the printed hearing record. Oral statements and answers to Member questions will be printed as part of the record of the hearing; only technical, grammatical, and typographical errors will be corrected. In order to allow sufficient time for questions at the hearing, you should highlight the most significant points in your testimony in an oral presentation of no more than five minutes.

Witnesses testifying before the Committee on Science, Space, and Technology must observe the procedures governing witness testimony. These procedures are described in the following enclosures and provide important details concerning the preparation and presentation of your testimony before the Committee on Science, Space, and Technology on November 19, 2013, at 10:00 a.m.:

Mr. Park
October 31, 2013
Page two

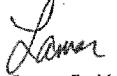
- The first enclosure outlines the rules governing appearance before the Committee.
- The second enclosure provides you with the Committee's Hearing Room Capabilities.
- The third enclosure provides you with the Truth-in-Testimony Instructions and the Truth-in-Testimony Disclosure Form.

Please email your testimony, biography, and truth in testimony form to Ms. Sarah Grady at Sarah.Grady@mail.house.gov as soon as it is available, but not less than 48 hours before the hearing. Sixty-five copies of your testimony must also be hand delivered to the Committee's main office, Room 2321 Rayburn Office Building, 48 hours prior to the hearing. Due to increased security measures in place at House office buildings, you will need to contact Ms. Grady to arrange for delivery of your testimony at (202) 225-6371.

In addition, if you wish to use the Committee's multimedia facilities during your oral testimony, a description of which is enclosed, please contact Mr. David Hartzler at david.hartzler@mail.house.gov. Our staff can usually accommodate most requests with 72 hours' notice.

If you have any questions concerning any aspect of your testimony, please contact Mr. Raj Bharwani, Committee on Science, Space, and Technology, at (202) 225-6371. I look forward to your participation in the hearing.

Sincerely,


Lamar Smith
Chairman

Enclosures (1) Rules Governing Appearance before the Committee on Science, Space, and Technology
(2) Hearing Room Capabilities
(3) Truth-In-Testimony Instructions and Truth-In-Testimony Disclosure Form

cc: Rep. Eddie Bernice Johnson
Ranking Member

MEMORANDUM

TO: WITNESSES APPEARING BEFORE THE SUBCOMMITTEE ON OVERSIGHT OF THE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY DURING THE 113th CONGRESS

FROM: COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

RE: RULES GOVERNING APPEARANCE BEFORE THE SUBCOMMITTEE

The following procedures govern witnesses appearing before the Committee on Science, Space, and Technology for the 113th Congress:

1. The Rules of the Committee require you to complete the attached **Truth-In-Testimony Disclosure Form** to disclose the amount and source (by agency and program) of any Federal grant (or subgrant thereof) or contract (or subcontract thereof) received during the current fiscal year or either of the two previous fiscal years by you or by an entity represented by you which are relevant to the subject matter of your testimony or the hearing at which you are testifying. Should you need extra space, please provide additional information on a separate sheet of paper.
2. You must submit to the Committee a **draft copy of your written testimony no less than 72 hours**, excluding weekends and Federal holidays, before you are to testify.
3. **No less than 48 hours**, excluding weekends and Federal holidays, before you are to testify, you must also submit to the Committee:
 - An **electronic copy of your final written testimony**, preferably in searchable PDF format, including any supporting graphs, charts, or slideshows. This electronic version will be posted on the Committee website, and will be accessible by the public.
 - **Forty-five (45) hard copies of your final written testimony**, including any supporting graphs, charts, or materials;
 - An **electronic copy of a short narrative biography**;
 - **Forty-five (45) hard copies of a short narrative biography**;

Enclosure 1

- **Two (2) hard copies of your Curriculum Vitae;** and
 - **Two (2) hard copies, including one signed original, of your completed Truth-In-Testimony Disclosure Form.**
5. You must notify the Committee **no later than 48 hours** before you are to testify **if you want to use any multimedia capabilities** as provided by the hearing room, and must provide all material to be presented in this fashion in hard copy form to the Committee. Please see *Enclosure 2* for further explanation of hearing room capabilities.
- If you are using any of the room's multimedia capabilities, you or your designee **must arrive no less than 30 minutes before the designated start time of the hearing** to allow for set-up. Failure to do so may result in the multimedia portion of the presentation being canceled.
6. Transcripts of hearings conducted by the Committee shall be published in substantially verbatim form, subject only to technical, grammatical, and typographical corrections:

NOTE: Section 210 of the Congressional Accountability Act of 1995 applies the rights and protections covered under the Americans with Disabilities Act of 1990 to the United States Congress. Accordingly, the Committee on Science and Technology strives to accommodate / meet the needs of those requiring special assistance. If you need special accommodation or require materials in alternative formats, please contact the Committee on Science and Technology in advance of the scheduled event (3 days requested) by telephone at (202) 225-6371, by facsimile at (202) 226-0113, or TTY (202) 226-4410.

**COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HEARING ROOM CAPABILITIES**

Equipment Capabilities

- A) PROJECTOR—The hearing room is equipped with a ceiling-mounted projector capable of displaying computer graphics and video feed.
- B) DROP DOWN VIDEO SCREEN—The rear of the hearing room is equipped with a large drop down screen viewable from the dais and side seats.
- C) WALL-MOUNTED LCD MONITORS—The hearing room is equipped with two monitors, one on each side of the room, for audience viewing.
- D) WITNESS MONITOR – A monitor will also be in place in front of the witness table so witnesses can see the screen, as well.

Computer- Based Presentation

Please bring your presentation on a memory stick (flash drive, thumb drive) or on your personal laptop to the hearing room at least a half-hour before the hearing so that we may help you set it up at the witness table. If you bring your presentation on a laptop, your laptop should be equipped with a functioning graphics port with either a VGA or MAC external connector. Because there are many makes and models of laptops, please be prepared to operate the external graphics port for your own laptop.

Audiovisual/Multimedia Capabilities

- A) The room supports the following transmission methods to broadcast committee activities to remote sites:
 - 1. Telephone Conferencing (Audio Only).
 - 2. Live Audio-Video Streaming (Webcasting).
 - 3. Video Teleconferencing.
 - 4. Video and Audio overflow transmission to room 2325.
- B) The room receives House Cable TV feeds for display.
- C) The hearing room equipment can playback and display compact discs, dvd discs, and overhead slides.

Equipment Support

Questions should be directed to David Hartzler at david.hartzler@mail.house.gov.

INSTRUCTIONS FOR COMPLETING THE TRUTH-IN-TESTIMONY DISCLOSURE FORM

In General. The accompanying form is intended to assist witnesses appearing before the Committee on Science, Space, and Technology Subcommittee on Oversight in complying with Rule XI, clause 2(g)(5) of the Rules of the House of Representatives. The rule requires that:

In the case of a witness appearing in a nongovernmental capacity, a written statement of proposed testimony shall include a curriculum vitae and a disclosure of the amount and source (by agency and program) of any Federal grant (or subgrant thereof) or contract (or subcontract thereof) received during the current fiscal year or either of the two previous fiscal years by the witness or by an entity represented by the witness. Such statements, with appropriate redactions to protect the privacy of the witness shall be made publicly available in electronic form not later than one day after the witness appears.

Please complete the form in accordance with these directions.

1. ***Name (Item 1 on the form).*** Please provide the name of the witness in the box at the top of the form.
2. ***Governmental Entity (Item 2).*** Please check the box indicating whether or not the witness is testifying on behalf of a government entity, such as a Federal department or agency, or a State or local department, agency, or jurisdiction. Trade or professional associations of public officials are not considered to be governmental organizations.
3. ***Nongovernmental Entity (Item 3).*** Please check the box indicating whether or not the witness is testifying on behalf of an entity that is not a governmental entity.
4. ***Entity(ies) to be Represented (Item 4).*** Please list all entities on whose behalf the witness is testifying.
5. ***Grants and Contracts (Item 5).*** Please list any Federal grants or contracts (including subgrants or subcontracts) that the witness personally or the entity the witness is representing has received from the Federal Government on or after October 1, 2010.
6. ***Representational Capacity (Item 6).*** If the answer to the question in item 2 is yes, please characterize the capacity in which the witness is testifying on behalf of the entities listed in item 4.
7. ***Affiliated Entities (Item 7).*** Please indicate whether the entity on whose behalf the witness is testifying has parent organizations, subsidiaries, or partnerships that are not represented by the testimony of the witness.
8. ***Grants and Contracts (Item 8).*** Please disclose grants and contracts as directed.
9. ***Submission.*** Please sign and date the form in the appropriate place. Please submit this form with your written testimony. Please note that under the Committee's rules, copies of a written statement of your proposed testimony must be submitted before the commencement of the hearing. To the greatest extent practicable, please also provide a copy in electronic format, preferably in searchable pdf format. Written testimony and the Truth-In-Testimony

Enclosure 3

disclosure form will be made publicly available and posted on the Committee's website.

Committee on Science, Space, and Technology

U.S. House of Representatives

Witness Disclosure Requirement - "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

1. Your Name:		
2. Are you testifying on behalf of the Federal, or a State or local government entity?	Yes	No
3. Are you testifying on behalf of an entity that is not a government entity?	Yes	No
4. Other than yourself, please list which entity or entities you are representing:		
5. Please list any Federal grants or contracts (including subgrants or subcontracts) that you or the entity you represent have received on or after October 1, 2010:		
6. If your answer to the question in item 3 in this form is "yes," please describe your position or representational capacity with the entity(ies) you are representing:		
7. If your answer to the question in item 3 is "yes," do any of the entities disclosed in item 4 have parent organizations, subsidiaries, or partnerships that you are not representing in your testimony?	Yes	No
8. If the answer to the question in item 3 is "yes," please list any Federal grants or contracts (including subgrants or subcontracts) that were received by the entities listed under the question in item 4 on or after October 1, 2010, that exceed 10 percent of the revenue of the entities in the year received, including the source and amount of each grant or contract to be listed:		

I certify that the above information is true and correct.

Signature: _____ Date: _____

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

November 26, 2013

The Honorable Lamar S. Smith
Chairman
House Committee on Science, Space, and Technology
2321 Rayburn HOB
Washington, D.C. 20515

Dear Chairman Smith:

Thank you for your phone call on Wednesday, which followed up on your letter of November 18, 2013. It was a pleasure speaking with you.

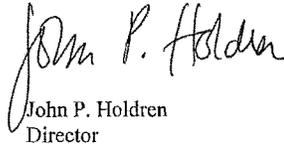
In our conversation and in your letter, you mentioned the Committee on Science, Space, and Technology's December 5th hearing regarding the security standards and technical measures to protect personal information on the healthcare.gov website. You asked that I encourage Todd Park to testify before the Committee on this topic.

As I understand my staff explained in response to your earlier invitation, neither Mr. Park nor any other Office of Science and Technology Policy (OSTP) staff member is in a position to testify on the data-security standards of the healthcare.gov website, as OSTP has not been substantially involved in developing those standards. Mr. Park previously testified that he has not focused on those issues and suggested that the Centers for Medicare and Medicaid Services (CMS) security team is in a better position to answer such questions.

Further, as you know, longstanding OSTP policy ordinarily permits only Senate-confirmed staff to testify before Congress. While Mr. Park is part of OSTP's leadership, he is not Senate-confirmed. Our current staff consists of two Senate-confirmed individuals: OSTP Associate Director for National Security and International Affairs Patricia Falcone and me. In our conversation, I offered that Dr. Falcone would be willing to testify on general cybersecurity policy issues, although she would not be able to comment specifically on the data-security standards for healthcare.gov. Should you decide to invite Dr. Falcone to testify, I request that the hearing take place after December the 9th because of scheduling conflicts during the first week of December.

Thank you again for taking the time to talk with me on Wednesday. I value our relationship and hope we will continue to have open discussions on issues before the Committee. As you know, I have testified before the Committee three times this year, and I remain committed to working with you on science and technology issues.

Sincerely,



John P. Holdren
Director

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member

THE WHITE HOUSE
WASHINGTON

November 17, 2014

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Smith and Chairman Broun:

I am following up on my letter of November 14, 2014, to address the substantial progress that has been made among our staffs in addressing the Committee on Science, Space, and Technology's interest in information concerning the healthcare.gov website and former United States Chief Technology Officer Todd Park. In just two months after the Committee asked to receive additional documents, the Office of Science and Technology Policy (OSTP) has produced over 8,000 pages of documents to the Committee. That is in addition to the more than 1,000 pages the Committee received earlier this year from OSTP, and the 1,324 pages of documents delivered to the Committee from among the materials produced to Congress by the Department of Health and Human Services. In addition to the 10,000-plus pages of documents the Committee has received, Mr. Park made himself available for a meeting with both of you in June to answer any questions. Mr. Park will also testify at a hearing before the Oversight Subcommittee this week, a hearing that he had agreed to attend voluntarily by letter dated September 16, 2014.

With respect to the Committee's document requests, the progress our staffs have made is encouraging. As you are aware, there exists an important and longstanding tradition by which Congress and the Executive, two co-equal branches of government, seek to accommodate the legitimate needs of one another. That tradition finds its roots in the Constitution itself, an "implicit constitutional mandate to seek optimal accommodation through a realistic evaluation of the needs of the conflicting branches in the particular fact situation." *United States v. American Tel. & Tel. Co.*, 567 F.2d 121, 127 (D.C. Cir. 1977).

In prior correspondence, we have explained that certain of the Committee's requests for information have run up against long-recognized Executive Branch confidentiality interests. As

Administrations of both political parties have long explained, if the Executive Branch is to function as the Constitution intends, it is imperative that White House advisers feel at liberty to have free and open deliberations and discussions, and that liberty frequently depends upon the expectation of confidentiality.

The Committee has consistently articulated an interest underlying its information requests, namely, the effort “to examine the safety, security and privacy of Americans’ personal data through the Obamacare website.”¹ More recently, the Committee has elaborated on that interest in security, stating that the Committee’s “jurisdiction over the Federal Information Security Management Act and the National Institute of Standard and Technology conveys to our Committee oversight over the security and implementation of Healthcare.gov.”²

The Executive Branch has made substantial efforts to accommodate the Committee’s articulated oversight interest consistent with its own constitutional and statutory responsibilities. As explained in prior correspondence, OSTP has produced documents based on the priorities articulated by Subcommittee staff. Specifically, OSTP expedited the production of documents from the time period that your staff indicated is of greatest interest to the Committee -- April 1, 2013, to October 1, 2013. A very small proportion of the documents produced to the Committee on October 10 and October 31, 2014, contained limited redactions in service of Executive Branch’s confidentiality interests. For the 30 redacted documents your staff identified as of interest, we have been able to make appropriate accommodations to provide your staff with access to additional information, including, in many cases, *in camera* review of fully unredacted materials; indeed, for those documents, there has not been one on which we have refused to make an additional accommodation. We have also agreed to the extraordinary step of allowing your staff to have temporary possession of certain of these documents solely for your non-public use in preparing members of the House Science Oversight Subcommittee who may participate in this week’s hearing.

As explained in prior correspondence, we also identified a small subset of materials that implicate longstanding Executive Branch interests that initially were not produced in prior document productions. Here too we have made significant and in some cases extraordinary accommodations to address your articulated information needs. In consultation with your staff, we identified via an electronic term search 17 documents that arguably touch on the security of the website. We have already offered accommodations on nearly all of these materials, agreeing to produce some to the Committee with limited redactions and allowing your staff to inspect others *in camera*. Furthermore, when your staff expressed a new desire for information concerning testing and the functionality of the website, we agreed to consider potential

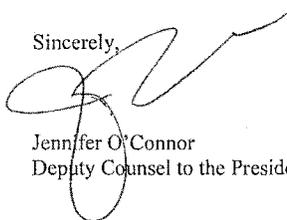
¹ Letter from the Hon. Lamar Smith, Paul Broun, M.D., and Larry Bucshon, M.D., to the Hon. John P. Holdren, Director, Office of Science and Technology Policy (December 20, 2013) [hereinafter “December 20 Letter”], at 3. Put in even greater detail, when Chairman Smith initially wrote to Mr. Park to express interest in healthcare.gov, the letter asked Mr. Park to address “what specific security standards and technical measures are in place to protect Americans’ privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or leaked.” Letter from the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology, to Todd Park, Assistant to the President and United States CTO (October 31, 2013), at 1.

² Email from H. Comm. on Science, Space, & Technology Majority Staff to White House Counsel’s Office staff (Nov. 12, 2014, 7:35 p.m.)

accommodations we might offer to provide additional information with the goal of reaching a mutually agreeable resolution of the Committee's outstanding document requests. I expect we will be able to have further productive discussions on these documents.

Thus, notwithstanding the extremely broad subpoena issued by the Committee, we have substantially narrowed the gap between our respective interests in the documents. The efforts we have made to do so reflect our deep commitment to cooperating with Congressional requests for information to the fullest extent consistent with the constitutional and statutory responsibilities of the Executive Branch. We look forward to continued progress in our discussions.

Sincerely,



Jennifer O'Connor
Deputy Counsel to the President

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Dan Maffei
Ranking Minority Member
Subcommittee on Oversight

THE WHITE HOUSE
WASHINGTON

November 14, 2014

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Smith and Chairman Broun:

I write in further response to the Committee on Science, Space, and Technology's interest in information concerning the healthcare.gov website and former United States Chief Technology Officer Todd Park. Enclosed with this letter are an additional 573 pages of documents that are responsive to the document subpoenas issued by the Subcommittee. One attachment that would otherwise have been included in the production did not render effectively. That document will be separately made available to the Committee for review.

This production further demonstrates OSTP's commitment foster a productive working relationship with the Committee and to satisfy the Committee's request for information, consistent with the interests of the Executive Branch. In addition, I am aware that our staffs have been meeting to discuss certain documents identified during the review of records thus far that implicate long-recognized Executive Branch confidentiality interests and have been pleased to learn that they have made steady progress towards identifying appropriate accommodations with respect to those documents. I trust that those meetings will continue in the same collaborative spirit moving forward.

Sincerely,



Jennifer O'Connor
Deputy Counsel to the President

Enclosure (documents Bates numbered OSTP ACA 8588-OSTP ACA 9160)

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Dan Maffei
Ranking Minority Member
Subcommittee on Oversight

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

www.science.house.gov

November 18, 2014

Honorable John P. Holdren, Director
Mr. Todd Park, U.S. Chief Technology Officer
Office of Science and Technology Policy
Executive Office of the President
725 17th Street NW
Washington, DC 20502

Dear Dr. Holdren and Mr. Park,

For over a year, the Committee on Science, Space, and Technology (Committee) has patiently and persistently sought information from the Office of Science and Technology Policy (OSTP) regarding its role in Helathcare.gov. As stated in our October 31, 2013, letter to Mr. Park, our interests began with the "lack of privacy standards for personal information passing through the Healthcare.gov website and the threat posed to Americans if hackers on the Internet gained access to such information."

The Committee sought further information about the role of Mr. Park and OSTP in this regard in a letter in December 2013 and received some limited information in January 2014. In July of 2014, the Committee received additional documents from the House Committee on Oversight and Government Reform (OGR) that they had obtained through their own inquiries. These documents suggested a much more extensive role by Mr. Park and OSTP personnel in the Healthcare.gov website than was previously conveyed to the Committee. Consequently, the originally stated interest was expanded after the Committee received these documents that demonstrated Mr. Park's *actual* role was decidedly different than what he testified to before OGR on November 13, 2013.

Over the course of the past year, the Committee repeatedly asked for Mr. Park to testify before the Committee. Unfortunately, these requests were re-buffed. Instead, OSTP offered for Mr. Park to brief the Committee on his role and responsibilities. This briefing would not be open to the public, but an opportunity for the Committee members to hear directly from Mr. Park. We had set a mutually agreed upon time for the briefing on September 10th, but OSTP reneged on its offer the night before after it learned that the briefing would be transcribed.

After multiple unsuccessful attempts to secure Mr. Park's testimony, the Committee was left no other choice but to subpoena both Mr. Park and all documents and communication that establish his

Dr. Holdren & Mr. Park
November 18, 2014
Page 2

actual involvement with Healthcare.gov. That subpoena demanded the production of any and all documents including communications that:

“...are related to the Healthcare.gov website, including but not limited to documents related to its hardware, software, design, testing, user capacity, operation, privacy protections, security, and problems, and also including but not limited to related contracts, reports, data submissions (including by contractors and insurers), and the federal data hub.”

I. Jurisdiction & Legislative Purpose.

Under House Rule X (1)(p), this Committee and its corresponding Subcommittee have jurisdiction over the OSTP and the National Institute for Standards and Technology (NIST). This Committee authorized the creation of the OSTP in 1976. This Committee has the authority to oversee the agencies responsible for setting cyber privacy and security policies and standards for the rest of the federal government including OSTP and NIST. In addition, under House Rule XI, the Committee is permitted to “conduct at any time such investigations and studies as it considers necessary or appropriate in the exercise of its responsibilities.”

As for the Committee’s legislative purpose, OSTP, through the Office of the White House Counsel (OWHC), has requested that we explain what our legitimate interests are for seeing the subpoenaed documents in an un-redacted format. The Committee’s jurisdiction over the Federal Information Security Management Act and the National Institute of Standards and Technology conveys to this Committee oversight over the security and implementation of Healthcare.gov.

The U.S. Supreme Court has unequivocally established that Congress’ power to conduct investigations and oversight is so essential to the legislative function that it may be implied from the general vesting of all legislative powers in Congress. In *McGrain v. Daugherty*, the Supreme Court described the power of inquiry, with the accompanying process to enforce it, as “an essential and appropriate auxiliary of to the legislative function.” (*McGrain*, 273 U.S. at 174-5.) The Court also noted that “[a] legislative body cannot legislate wisely or effectively in the absence of information respecting the conditions which the legislation is intended to affect or change.” (*Id.*)

In *Eastland v. United States Serviceman’s Fund*, the Court stipulated that the “scope of [Congress’s] power of inquiry ... is as penetrating and far-reaching as the potential power to enact and appropriate under the Constitution.” (*Eastland*, 421 U.S. at 504 n.15 (quoting *Barenblatt*, 360 U.S. at 111). The Court has also described Congressional power as “broad,” “indispensable,” and “encompassing inquiries concerning the administration of existing laws as well as proposed or possible needed statutes.” (*Watkins*, 354 U.S. at 187.)

Absent an express statutory restriction, federal courts have held that executive agencies may not refuse to provide information to Congress, even if such information is confidential, proprietary, or otherwise barred from being disclosed to the public. (*F.T.C. v. Owens-Corning Fiberglass Corp.*, 626 F.2d 966, 970 (D.C. Cir. 1980); *Exxon Corp.*, 589 F.2d at 585-6; *Ashland Oil*, 548 F.2d at 979).

Dr. Holdren & Mr. Park
November 18, 2014
Page 3

Based on the issues surrounding its rollout, Congress has a responsibility to review the standards that were used to ensure its security and functionality to the American people. However, to properly conduct our legislative and oversight responsibilities, we have to depend on the veracity of those that have provided Congress with information. Any misinformation given to Congress impedes our constitutional ability to formulate a response. Based on emails and other documents received by the Committee, we have reason to believe that OSTP's correspondence to the Committee and Mr. Park's testimony before OGR has not been forthcoming about Mr. Park's involvement in Healthcare.gov and such misinformation impedes this Committee's ability to conduct oversight and respond to the problems associated with the website.

II. OSTP's Failure to Comply

Since the duly issued and served subpoena on September 19, 2014, the Committee has received thousands of documents. However, responsiveness is not measured by the number of pages produced, but by completely fulfilling the requests from Congress. Sending multiple copies of long documents, many with questionable redactions, is not cooperating with the process but is a tactic used to confuse and delay the Committee's oversight. OSTP's response to this legitimate exercise of Congressional oversight authority has been disappointing. Instead of prompt compliance, there has been a pattern of dilatory tactics from the onset of this oversight inquiry.

The subpoena itself is broad in the sense of the types of documents sought, but quite narrow in that they all focus on Todd Park's role with Healthcare.gov. Considering OSTP failed to provide all of the documents the Committee requested last December, it is the Committee's hope that the detailed list of documents sought will in full faith complete the inquiry in its entirety. Unfortunately, the breadth of the subpoena was in no small part a direct response to the lack of cooperation from OSTP and Congress' inability to get straight forward answers to legitimate oversight inquiries. Since the issuance of the subpoena almost two months ago, the Committee has gone to great lengths to accommodate OSTP by further prioritizing not only the subject matter, format, and date range of the subpoena, but also agreeing to an *in camera* review on more than one occasion with the OWHC in order to help receive documents in a somewhat timely fashion. It has therefore been disheartening to see the OWHC use this accommodation to exclude documents the Committee had clearly indicated it was interested in and again failed to produce the documents to the Committee in an un-redacted format.

While some progress has been made, despite nearly two months of effort, there are still specifically identified responsive emails that have yet to be provided even in a redacted format. Of those redacted documents that have been turned over, on numerous occasions my staff requested that they be produced in an un-redacted format or as an additional accommodation requested a detailed list of the documents identifying why they are redacted and providing not only a description of the redacted portion but also a legitimate legal basis for its redaction. Unfortunately, the OWHC has not been able to accommodate these requests thus far.

III. The claim of "Executive Branch confidentiality interest" is Without Merit

Dr. Holdren & Mr. Park
November 18, 2014
Page 4

To date, OSTP and OWHC have asserted only a generalized claim of a “long-standing Executive Branch confidentiality interest” as the rationale for refusing to provide some of the requested material. Congress also has a “long-standing legislative interest in oversight” and is entitled to review duly subpoenaed documents. As we have expressed multiple times, “Executive Branch confidentiality interests” are not a legal basis for withholding subpoenaed information from Congress. OSTP and OWHC have failed to provide a detailed privilege log identifying the documents being withheld in full or in part, and the legal basis that would justify applicability of a privilege to the withheld information. A general assertion of “Executive Branch confidentiality interests,” in the face of a duly authorized Congressional subpoena, is neither a constitutionally protected privilege nor even a recognized common law privilege. The general interests discussed have historically been in response to a Congressional *request* for information. However, at least since its drafting in 1989 by Assistant Attorney General William Barr, the Executive Branch distinguishes the generalized claim of “Executive Branch confidentiality interests” in response to a Congressional request much differently than in response to a duly authorized Congressional subpoena.

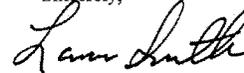
“While the considerations that support the concept and assertion of executive privilege apply to any congressional request for information, the privilege itself need not be claimed formally vis-s-vis Congress **except** in response to a lawful subpoena...” Memorandum for Congressional Requests for Confidential Executive Branch Information, June 19, 1989 (Emphasis added)

If it is OSTP’s position that “Executive Branch confidentiality interests” outweigh Congressional oversight and legislative interests, then we request that you inform the Committee whether executive privilege is being asserted by the President and whether the basis of that assertion is some form of “deliberative process” or “presidential communication.” If executive privilege is in fact asserted, then the Committee is entitled to a written summary of the redacted portions so that we can determine our next course of action.

IV. Compliance with Duly Authorized Subpoena

Given that the Committee began this oversight well over a year ago and the subpoena was issued nearly two months ago, the time for accommodation and dilatory tactics must come to an end. The Committee demands, through the authority of the aforementioned duly authorized Congressional subpoena, that any and all responsive documents, and in particular those that have been specifically identified by Committee staff, be turned over to this Committee immediately in an un-redacted format.

Sincerely,



Lamar Smith
Chairman

Cc: Rep. Eddie Bernice Johnson
Ranking Member

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

July 3, 2014

The Honorable Paul Broun
Chairman, Subcommittee on Oversight
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Broun,

Thank you for meeting with Congressmen Smith, Wolf, and Fattah, U.S. Chief Technology Officer (CTO) Todd Park, and me on June 24, 2014. We appreciated the opportunity to meet with you.

At that meeting, you and Chairman Smith reiterated that the Subcommittee's oversight interest continues to be the security and privacy of the Healthcare.gov website. When Mr. Park offered to answer questions and clarify his role, you responded that you were not there to get answers, and you indicated that you felt all of the Subcommittee members should have a chance to ask questions. We accordingly write to follow up on our meeting and to continue the efforts we have made to try and accommodate the Subcommittee's stated oversight interests.

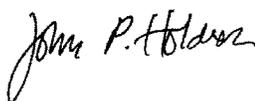
The Office of Science and Technology Policy's (OSTP) prior correspondence with Chairman Smith makes clear that Mr. Park and OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace's (FFM) security measures. In attempting to arrive at an appropriate accommodation, this is worth emphasizing. Mr. Park is not a cybersecurity expert; he did not develop or approve the security measures in place to protect the website, and he does not manage those responsible for keeping the site safe. The Centers for Medicare and Medicaid Services are directly responsible for those tasks and have the relevant first-hand knowledge.

Nevertheless, OSTP has tried to provide information to meet your stated interest and that of the Committee, including by offering Dr. Patricia Falcone, a Senate-confirmed Associate Director, to testify regarding cybersecurity issues generally. As a further significant attempt to accommodate your stated interests, OSTP is willing to arrange for Mr. Park to meet with the Oversight Subcommittee members at a mutually convenient time. Mr. Park would brief members about his role as CTO and members would have an opportunity to ask Mr. Park questions about the extent of his familiarity with the security and privacy aspects of the Healthcare.gov website. Associate Director Falcone would also be willing to attend such a meeting with Mr. Park. Dr. Falcone does not have specific knowledge of the data-security standards in place for healthcare.gov, but she is knowledgeable about general cybersecurity

policy issues, including a cybersecurity report that your staff identified as relevant to its inquiry when first seeking an OSTP witness to testify before the Committee.

Finally, you asked for a list of the CTO Office's staff and the salaries OSTP pays. The CTO Office's staff is listed on OSTP's webpage: <http://www.whitehouse.gov/administration/eop/ostp/about/leadershipstaff>. OSTP pays four of these staff members and, in the aggregate, the salary expenses total \$456,418. OSTP looks forward to continuing to work with you on science and technology issues.

Sincerely,



John P. Holdren
Assistant to the President for Science and Technology
Director, Office of Science and Technology Policy

cc: The Honorable Lamar Smith
Chairman
Committee on Science, Space and Technology

The Honorable Frank Wolf
Chairman
Subcommittee on Commerce, Justice, and Science

The Honorable Chaka Fattah
Ranking Member
Subcommittee on Commerce, Justice, and Science

The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space and Technology

The Honorable Dan Maffei
Ranking Member, Subcommittee on Oversight
Committee on Science, Space, and Technology

* Email from H. Comm. on Science, Space, & Technology Majority Staff to OSTP staff (Oct. 28, 2013, 5:42 p.m.) ("I suspect we would touch on related issues raised and addressed in the 'Cyberspace Policy Review' and the Dec. 2011 report 'Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,' both of which were referred to in Dr. Holdren's testimony before the Committee in a full committee oversight hearing on June 20, 2012.")

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

October 31, 2013

Mr. Todd Park
Chief Technology Officer
Office of Science and Technology Policy
725 17th Street, N.W.
Washington, DC 20502

Dear Mr. Park:

On Tuesday November 19, 2013, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building, the Committee on Science, Space, and Technology will hold a hearing titled, "Is Your Data on the Healthcare.gov Website Secure?" I am writing to formally invite you to testify at this hearing.

The hearing will examine concerns about the lack of privacy standards for personal information passing through the Healthcare.gov website and the threat posed to Americans if hackers on the Internet gained access to such information.

The data passing through the Healthcare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. In order to gain information on potential healthcare coverage through the website, users must input personal contact information, birth dates and social security numbers for all family members, as well as household salary and debt information. Users may also be asked to verify home mortgage and credit card information, place of employment, previous addresses, and whether the person has any physical or mental disabilities.

In your testimony, please be prepared to discuss what specific security standards and technical measures are in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or leaked.

You are requested to submit a written statement, which may be of any reasonable length and may contain supplemental materials; however, please be aware that the Committee cannot guarantee that supplemental material will be included in the printed hearing record. Oral statements and answers to Member questions will be printed as part of the record of the hearing; only technical, grammatical, and typographical errors will be corrected. In order to allow sufficient time for questions at the hearing, you should highlight the most significant points in your testimony in an oral presentation of no more than five minutes.

Witnesses testifying before the Committee on Science, Space, and Technology must observe the procedures governing witness testimony. These procedures are described in the following enclosures and provide important details concerning the preparation and presentation of your testimony before the Committee on Science, Space, and Technology on November 19, 2013, at 10:00 a.m.:

Mr. Park
October 31, 2013
Page two

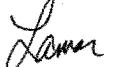
- The first enclosure outlines the rules governing appearance before the Committee.
- The second enclosure provides you with the Committee's Hearing Room Capabilities.
- The third enclosure provides you with the Truth-in-Testimony Instructions and the Truth-in-Testimony Disclosure Form.

Please email your testimony, biography, and truth in testimony form to Ms. Sarah Grady at Sarah.Grady@mail.house.gov as soon as it is available, but not less than 48 hours before the hearing. Sixty-five copies of your testimony must also be hand delivered to the Committee's main office, Room 2321 Rayburn Office Building, 48 hours prior to the hearing. Due to increased security measures in place at House office buildings, you will need to contact Ms. Grady to arrange for delivery of your testimony at (202) 225-6371.

In addition, if you wish to use the Committee's multimedia facilities during your oral testimony, a description of which is enclosed, please contact Mr. David Hartzler at david.hartzler@mail.house.gov. Our staff can usually accommodate most requests with 72 hours' notice.

If you have any questions concerning any aspect of your testimony, please contact Mr. Raj Bharwani, Committee on Science, Space, and Technology, at (202) 225-6371. I look forward to your participation in the hearing.

Sincerely,



Lamar Smith
Chairman

Enclosures (1) Rules Governing Appearance before the Committee on Science, Space, and Technology
(2) Hearing Room Capabilities
(3) Truth-In-Testimony Instructions and Truth-In-Testimony Disclosure Form

cc: Rep. Eddie Bernice Johnson
Ranking Member

Enclosure 1

MEMORANDUM

TO: WITNESSES APPEARING BEFORE THE **SUBCOMMITTEE ON OVERSIGHT OF THE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY DURING THE 113th CONGRESS**

FROM: COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

RE: RULES GOVERNING APPEARANCE BEFORE THE SUBCOMMITTEE

The following procedures govern witnesses appearing before the Committee on Science, Space, and Technology for the 113th Congress:

1. The Rules of the Committee require you to complete the attached **Truth-In-Testimony Disclosure Form** to disclose the amount and source (by agency and program) of any Federal grant (or subgrant thereof) or contract (or subcontract thereof) received during the current fiscal year or either of the two previous fiscal years by you or by an entity represented by you which are relevant to the subject matter of your testimony or the hearing at which you are testifying. Should you need extra space, please provide additional information on a separate sheet of paper.
2. You must submit to the Committee a **draft copy of your written testimony no less than 72 hours**, excluding weekends and Federal holidays, before you are to testify.
3. **No less than 48 hours**, excluding weekends and Federal holidays, before you are to testify, you must also submit to the Committee:
 - An **electronic copy of your final written testimony**, preferably in searchable PDF format, including any supporting graphs, charts, or slideshows. This electronic version will be posted on the Committee website, and will be accessible by the public.
 - **Forty-five (45) hard copies of your final written testimony**, including any supporting graphs, charts, or materials;
 - An **electronic copy of a short narrative biography**;
 - **Forty-five (45) hard copies of a short narrative biography**;

Enclosure 1

- **Two (2) hard copies of your Curriculum Vitae; and**
 - **Two (2) hard copies, including one signed original, of your completed Truth-In-Testimony Disclosure Form.**
5. You must notify the Committee **no later than 48 hours** before you are to testify if you **want to use any multimedia capabilities** as provided by the hearing room, and must provide all material to be presented in this fashion in hard copy form to the Committee. Please see *Enclosure 2* for further explanation of hearing room capabilities.
- If you are using any of the room's multimedia capabilities, you or your designee **must arrive no less than 30 minutes before the designated start time of the hearing** to allow for set-up. Failure to do so may result in the multimedia portion of the presentation being canceled.
6. Transcripts of hearings conducted by the Committee shall be published in substantially verbatim form, subject only to technical, grammatical, and typographical corrections.

NOTE: Section 210 of the Congressional Accountability Act of 1995 applies the rights and protections covered under the Americans with Disabilities Act of 1990 to the United States Congress. Accordingly, the Committee on Science and Technology strives to accommodate / meet the needs of those requiring special assistance. If you need special accommodation or require materials in alternative formats, please contact the Committee on Science and Technology in advance of the scheduled event (3 days requested) by telephone at (202) 225-6371, by facsimile at (202) 226-0113, or TTY (202) 226-4410.

**COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HEARING ROOM CAPABILITIES**

Equipment Capabilities

- A) PROJECTOR—The hearing room is equipped with a ceiling-mounted projector capable of displaying computer graphics and video feed.
- B) DROP DOWN VIDEO SCREEN—The rear of the hearing room is equipped with a large drop down screen viewable from the dais and side seats.
- C) WALL-MOUNTED LCD MONITORS—The hearing room is equipped with two monitors, one on each side of the room, for audience viewing.
- D) WITNESS MONITOR – A monitor will also be in place in front of the witness table so witnesses can see the screen, as well.

Computer- Based Presentation

Please bring your presentation on a memory stick (flash drive, thumb drive) or on your personal laptop to the hearing room at least a half-hour before the hearing so that we may help you set it up at the witness table. If you bring your presentation on a laptop, your laptop should be equipped with a functioning graphics port with either a VGA or MAC external connector. Because there are many makes and models of laptops, please be prepared to operate the external graphics port for your own laptop.

Audiovisual/Multimedia Capabilities

- A) The room supports the following transmission methods to broadcast committee activities to remote sites:
 - 1. Telephone Conferencing (Audio Only).
 - 2. Live Audio-Video Streaming (Webcasting).
 - 3. Video Teleconferencing.
 - 4. Video and Audio overflow transmission to room 2325.
- B) The room receives House Cable TV feeds for display.
- C) The hearing room equipment can playback and display compact discs, dvd discs, and overhead slides.

Equipment Support

Questions should be directed to David Hartzler at david.hartzler@mail.house.gov.

INSTRUCTIONS FOR COMPLETING THE TRUTH-IN-TESTIMONY DISCLOSURE FORM

In General. The accompanying form is intended to assist witnesses appearing before the Committee on Science, Space, and Technology Subcommittee on Oversight in complying with Rule XI, clause 2(g)(5) of the Rules of the House of Representatives. The rule requires that:

In the case of a witness appearing in a nongovernmental capacity, a written statement of proposed testimony shall include a curriculum vitae and a disclosure of the amount and source (by agency and program) of any Federal grant (or subgrant thereof) or contract (or subcontract thereof) received during the current fiscal year or either of the two previous fiscal years by the witness or by an entity represented by the witness. Such statements, with appropriate redactions to protect the privacy of the witness shall be made publicly available in electronic form not later than one day after the witness appears.

Please complete the form in accordance with these directions.

1. ***Name (Item 1 on the form).*** Please provide the name of the witness in the box at the top of the form.
2. ***Governmental Entity (Item 2).*** Please check the box indicating whether or not the witness is testifying on behalf of a government entity, such as a Federal department or agency, or a State or local department, agency, or jurisdiction. Trade or professional associations of public officials are not considered to be governmental organizations.
3. ***Nongovernmental Entity (Item 3).*** Please check the box indicating whether or not the witness is testifying on behalf of an entity that is not a governmental entity.
4. ***Entity(ies) to be Represented (Item 4).*** Please list all entities on whose behalf the witness is testifying.
5. ***Grants and Contracts (Item 5).*** Please list any Federal grants or contracts (including subgrants or subcontracts) that the witness personally or the entity the witness is representing has received from the Federal Government on or after October 1, 2010.
6. ***Representational Capacity (Item 6).*** If the answer to the question in item 2 is yes, please characterize the capacity in which the witness is testifying on behalf of the entities listed in item 4.
7. ***Affiliated Entities (Item 7).*** Please indicate whether the entity on whose behalf the witness is testifying has parent organizations, subsidiaries, or partnerships that are not represented by the testimony of the witness.
8. ***Grants and Contracts (Item 8).*** Please disclose grants and contracts as directed.
9. ***Submission.*** Please sign and date the form in the appropriate place. Please submit this form with your written testimony. Please note that under the Committee's rules, copies of a written statement of your proposed testimony must be submitted before the commencement of the hearing. To the greatest extent practicable, please also provide a copy in electronic format, preferably in searchable pdf format. Written testimony and the Truth-In-Testimony

Enclosure 3

disclosure form will be made publicly available and posted on the Committee's website.

Committee on Science, Space, and Technology

U.S. House of Representatives

Witness Disclosure Requirement - "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

1. Your Name:		
2. Are you testifying on behalf of the Federal, or a State or local government entity?	Yes	No
3. Are you testifying on behalf of an entity that is not a government entity?	Yes	No
4. Other than yourself, please list which entity or entities you are representing:		
5. Please list any Federal grants or contracts (including subgrants or subcontracts) that you or the entity you represent have received on or after October 1, 2010:		
6. If your answer to the question in item 3 in this form is "yes," please describe your position or representational capacity with the entity(ies) you are representing:		
7. If your answer to the question in item 3 is "yes," do any of the entities disclosed in item 4 have parent organizations, subsidiaries, or partnerships that you are not representing in your testimony?	Yes	No
8. If the answer to the question in item 3 is "yes," please list any Federal grants or contracts (including subgrants or subcontracts) that were received by the entities listed under the question in item 4 on or after October 1, 2010, that exceed 10 percent of the revenue of the entities in the year received, including the source and amount of each grant or contract to be listed:		

I certify that the above information is true and correct.

Signature: _____ Date: _____

THE WHITE HOUSE
WASHINGTON

October 10, 2014

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairmen Smith and Broun:

I write in response to the Committee on Science, Space, and Technology's continued interest in information concerning the healthcare.gov website and former United States Chief Technology Officer Todd Park, including the subpoenas for documents issued on September 19, 2014. Before the Subcommittee on Oversight authorized issuance of the subpoenas, the Office of Science and Technology Policy (OSTP) produced more than one thousand pages of documents to the Committee and stated it was willing to produce additional documents voluntarily. In addition, Mr. Park attended a meeting with both of you in June to answer any questions, and he also offered to appear again and answer questions at a hearing in November. Despite these efforts to address the Committee's interests, the Subcommittee on Oversight elected to authorize the issuance of subpoenas.

The subpoenas issued by the Committee are quite broad. For nearly a year, the Committee consistently articulated its oversight interest in healthcare.gov as a desire for information about the measures in place to defend the HealthCare.gov website against malicious cyber attacks and to safeguard the personal data of Americans.¹ The subpoena resolution

¹ See, e.g., Letter from the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology, to Todd Park, Assistant to the President and United States CTO (October 31, 2013), at 1 (Mr. Park should address "what specific security standards and technical measures are in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or leaked."); Letter from the Hon. Lamar Smith, Paul Broun, M.D., and Larry Bucshon, M.D., to the Hon. John P. Holdren, Director, Office of Science and Technology Policy (December 20, 2013) (referencing a Committee hearing in November of that year to examine the risks that online criminals and identity thieves might pose if they gained access to customers' personal information); 160 Cong. Rec. H4953 (daily ed. May 29, 2014) (statement of Rep. Broun) ("It also turns out that a co-chairman of this Obamacare website Steering Committee is the U.S. Chief Technology Officer in the White

memorandum prepared for the Oversight Subcommittee, in a section discussing the questions that remain, makes clear that the Subcommittee sought “to have subpoenas issued to Mr. Park in order to compel his records and his appearance before the Oversight Subcommittee to answer questions regarding the security of the website”² The press release issued by the Committee after the vote to authorize the subpoenas, entitled “Subcommittee Votes to Subpoena Todd Park on White House Role in HealthCare.gov Security,” continued to emphasize the Committee’s interest in security.³

The actual terms of the Committee’s subpoenas, however, extend well beyond the Committee’s articulated interest in the security of the website. The subpoenas’ broad demands for the production of records “related to the HealthCare.gov website” intrude on Executive Branch interests, particularly in light of the substantial resources required to gather and review many documents that would appear to be of little, if any, oversight interest—for instance, news articles that simply mention HealthCare.gov or other materials unrelated to the security measures in place to protect the website.

As evidence of OSTP’s continued desire to foster a productive working relationship with the Committee, however, enclosed with this letter are 5,613 pages of documents that are responsive to the terms of the subpoenas as written. OSTP will continue to review and produce additional documents on a rolling basis to speed the Committee’s access to information. At the same time, I continue to encourage your staff to contact my staff to engage in the traditional process of dialog and accommodation that would allow us to explore ways in which the Committee might prioritize or narrow its requests for information and allow us to more efficiently work to satisfy the Committee’s particularized information needs.

Sincerely,



W. Neil Eggleston
Counsel to the President

House Office of Science and Technology Policy, Mr. Todd Park. Upon learning this, I, as chairman of the Oversight Subcommittee, along with full Committee Chairman Smith, and Research and Technology Subcommittee Chairman Dr. Bucshon, sent a December 20, 2013, letter to the White House requesting that Mr. Park make himself available to the committee to answer questions regarding the security issues with healthcare.gov by January 10.”)

² Memorandum from Oversight Subcommittee Staff to Members and Staff of the Science, Space, and Technology Subcommittee of Oversight (Sept. 12, 2014), at 6.

³ Subcommittee on Oversight of the Committee on Science, Space, & Technology Press Release, “Subcommittee Votes to Subpoena Todd Park on White House Role in HealthCare.gov Security,” Sept. 17, 2014 (“The Committee has invited Mr. Park to testify before us on five different occasions on his knowledge of privacy and security matters relating to the Affordable Care Act website, HealthCare.gov. . . . Additionally, recent reports about a successful hack of the website have further raised the stakes on the need to ensure Americans who log on to HealthCare.gov later this year are safe from cyber criminals.”).

Enclosure (documents Bates numbered 0001108-0006720)

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Dan Maffei
Ranking Minority Member
Subcommittee on Oversight

THE WHITE HOUSE
WASHINGTON

October 31, 2014

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

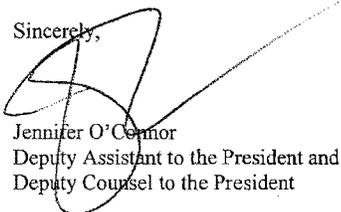
Dear Chairman Smith and Chairman Broun:

I write in further response to the Committee on Science, Space, and Technology's interest in information concerning the healthcare.gov website and former United States Chief Technology Officer Todd Park. The Office of Science and Technology Policy (OSTP) has produced over 6,500 pages of documents to the Committee to date. As requested, we also arranged for delivery to the Committee of 1,324 pages of documents sent or received by Todd Park from among the 130,000-plus pages of documents produced to Congress by the Department of Health and Human Services concerning healthcare.gov. To further accommodate your articulated interest, Mr. Park attended a meeting with both of you in June to answer any questions. OSTP has also repeatedly offered to have Associate Director Patricia Falcone testify at a Committee hearing on cybersecurity policy issues. Mr. Park also had voluntarily agreed to testify at a hearing next month before you issued an unnecessary subpoena to compel his attendance.

Enclosed with this letter are an additional 1,857 pages of documents that are responsive to the document subpoenas issued by the Subcommittee. In producing these materials, OSTP has made an effort to respond to the priorities articulated in discussions with Subcommittee staff. In addition to the materials produced with this letter, I invite your staff to contact Lamar Baker and Nicholas McQuaid of my staff next week to discuss how we might make further accommodations, including the possibility of *in camera* review, for documents identified during the review of records thus far that implicate long-recognized Executive Branch confidentiality interests. The ability to tailor appropriate accommodations would be aided by an explanation from the Committee of whether there exists a particularized need for such documents in light of the Committee's stated interest in the security measures in place to defend the healthcare.gov website against malicious cyber-attacks and to safeguard the personal data of Americans.

With the nearly 10,000 pages of documents the Committee has now received, Mr. Park's testimony in November, and the other efforts OSTP has made, much has already been accomplished to meet the Committee's articulated interest. OSTP will continue to work to accommodate the Committee's request in a manner that takes into account relevant time demands and the scheduled hearing date in November. To that end, in its review and processing of remaining documents that may be responsive to the very broad subpoenas issued by the Committee, OSTP intends to focus on materials created after October 1, 2013, that concern the security of healthcare.gov. OSTP expects to be in a position to make a next production of documents that includes such materials within two weeks. After the Committee receives those additional documents, our respective staffs will be in a better position to discuss any remaining legitimate interest in Mr. Park's role with respect to healthcare.gov and how best to accommodate any such interest consistent with the duties and responsibilities of the Executive Office of the President.

Sincerely,



Jennifer O'Connor
Deputy Assistant to the President and
Deputy Counsel to the President

Enclosure (documents Bates numbered 0006721-0008577)

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Dan Maffei
Ranking Minority Member
Subcommittee on Oversight

THE WHITE HOUSE
WASHINGTON

September 16, 2014

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Broun:

I understand that last Friday the Committee on Science, Space, and Technology's Subcommittee on Oversight (the Subcommittee) noticed a September 17, 2014, business meeting to consider issuing two subpoenas. As described in the notice, the Subcommittee will consider whether to issue a subpoena for Todd Park to appear at a hearing before the Subcommittee, and whether to issue a subpoena for the production of some of Mr. Park's records, during his former tenure in the Office of Science and Technology Policy (OSTP) as United States Chief Technology Officer (CTO), relating to the healthcare.gov website.

I write in advance of the Subcommittee's meeting to ensure you understand that the issuance of these subpoenas is unnecessary. Mr. Park will appear voluntarily for a hearing before the Subcommittee on a mutually convenient date in November to discuss your expressed interest in the healthcare.gov website. OSTP is willing to produce additional documents—including the 102 pages proactively provided with this letter—to further accommodate your "efforts to examine the safety, security and privacy of Americans' personal data through the [Obamacare](http://Obamacare.gov) website."¹ The remainder of this letter discusses OSTP's efforts to cooperate with your oversight interests thus far, and OSTP's continued willingness to do so without any need for subpoenas.

I understand that both the full Committee and the Oversight Subcommittee have articulated their interest in the security of healthcare.gov as a desire for information about the measures in place to defend the healthcare.gov website against malicious cyber attacks and to safeguard the personal data of Americans. When Chairman Smith initially wrote to Mr. Park to express interest in healthcare.gov, the letter asked Mr. Park to address "what specific security standards and technical measures are in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or

¹ Letter from the Hon. Lamar Smith, Paul Broun, M.D., and Larry Bucshon, M.D., to the Hon. John P. Holdren, Director, Office of Science and Technology Policy (December 20, 2013) [hereinafter "December 20 Letter"], at 3.

leaked.”² An email from Committee staff to OSTP at about the same time expressed interest in cybersecurity issues more generally, including a cybersecurity policy report that OSTP Associate Director Patricia Falcone helped prepare.³ In the same vein, your December 20, 2013, letter to OSTP referenced a hearing the Committee held in November of that year to examine the risks that online criminals and identity thieves might pose if they gained access to customers’ personal information.⁴ And more recently in January of this year, the Committee continued its focus on the standards and technical protocols in place to defend against malicious cyber attacks in a second hearing convened on the same topic with “white hat” hackers as witnesses.⁵

From the outset, OSTP has been clear about the limitations both it and Mr. Park face in attempting to respond to the requests for information and testimony concerning these issues involving the development of security standards and the design of scenarios to respond to malicious intrusion attempts. As noted several times in prior correspondence, primary responsibility for those tasks lies elsewhere—with the Centers for Medicare and Medicaid Services (CMS)—and it is CMS that is in the best position to provide complete, current, and accurate information regarding the security protocols in place to protect the website. Nevertheless, the record reflects that OSTP has made substantial efforts to try to accommodate the Committee’s interest in security and to clarify Mr. Park’s role.

OSTP has produced more than one thousand pages of documents; offered on multiple occasions to have Associate Director Falcone testify at a Committee hearing on cybersecurity policy issues; made Mr. Park available for a meeting with you and Chairman Smith in your office, where Mr. Park was willing to address any questions put to him; and offered to have Mr. Park brief all Subcommittee members. Through these substantial efforts at accommodation, OSTP has attempted to help the Committee better understand Mr. Park’s actual duties as the United States CTO and his role with respect to healthcare.gov.

In particular, regarding the documents you have received, your letter of December 20 asked OSTP to produce a very broad set of materials, including all OSTP records concerning the Affordable Care Act and healthcare.gov, scheduling information, records concerning internal White House briefings, and even documents that had not been created but might conceivably be provided to Congress in the future.⁶ Confronted with this broad request and a short deadline in the December 20 letter for responding, OSTP focused its efforts to provide information on the issue that was plainly of particular interest to the Committee, namely, Mr. Park’s participation as one of three co-chairs on the healthcare.gov Interagency Steering Committee. Your December

² Letter from the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology, to Todd Park, Assistant to the President and United States CTO (October 31, 2013), at 1.

³ Email from H. Comm. on Science, Space, & Technology Majority Staff to OSTP staff (Oct. 28, 2013, 5:42 p.m.) (“I suspect we would touch on related issues raised and addressed in the ‘Cyberspace Policy Review’ and the Dec 2011 report ‘Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,’ both of which were referred to in Dr. Holdren’s testimony before the Committee in a full committee oversight hearing on June 20, 2012.”)

⁴ December 20 Letter, at 1 (“The expert witnesses at our hearing outlined the significant risk of identity theft to Americans if hackers gained access to their personal information.”).

⁵ *Hearing Before the H. Comm. on Science, Space, & Tech.*, 113th Cong. (January 16, 2014) [hereinafter, January 16 Hearing].

⁶ December 20 Letter at 3.

20 letter focused on this Steering Committee and its security and privacy subgroup—even going so far as to attach a draft charter for the Steering Committee.⁷

Accordingly, in its January 15, 2014, response, OSTP described the documents it was producing: those concerning the Steering Committee and other interagency meetings that made reference to security, which appeared to be of special interest to the Committee.⁸ OSTP's January 15 letter also explained the interagency coordination function the Steering Committee served, Mr. Park's role in it, and why his participation was not an indication that he had substantial knowledge or expertise concerning the standards or technical protocols for dealing with malicious intrusions that are the focus of the Subcommittee's oversight inquiry. In the eight months following OSTP's production of these documents, the Subcommittee expressed no continued interest in receiving additional documents, nor did it raise any questions concerning the Steering Committee materials provided. Thus, you can understand why the abrupt notice of a business meeting to consider a subpoena for documents came as a surprise.

Despite OSTP's efforts at accommodation, it seems that the push to issue subpoenas this fall may unfortunately reflect a continued misunderstanding of Mr. Park's involvement in the security of the healthcare.gov website. This letter therefore provides additional information, namely, additional OSTP documents beyond those already provided concerning the Interagency Steering Committee, concerning Mr. Park's limited involvement in the security aspects of the website, which are primarily handled by CMS. The enclosed documents can be grouped into three categories.

First, in an extension of his role with the Steering Committee, Mr. Park, and his other co-Chairs were occasionally asked to assist in instances when White House personnel made requests to officials at HHS and CMS. One instance when such assistance was sought involved a request for a meeting on user credentialing and identity-proofing from National Security Staff and Office of Management and Budget officials. The documents themselves make clear that although the particular request for assistance was made from CMS officials to Mr. Park, it was another co-Chair who provided assistance in addressing that request.⁹

Second, Mr. Park was asked on a small number of occasions to assist in obtaining information from CMS and HHS personnel responsible for security of the website. In that role, Mr. Park asked HHS and CMS officials to develop background points describing the cybersecurity protections and helped coordinate follow-up conversations between the HHS and CMS officials and cybersecurity experts both inside and outside the government. Again, the emails themselves show that Mr. Park was not directly familiar with the development of

⁷ See also *January 16 Hearing* (statement of Rep. Paul Broun, M.D.) (“It’s probably [sic] the oversight committee of—subcommittee of this committee’s attention that there is—or at least was [an] Affordable Care Act information technology exchanges steering committee [chaired] by senior White House officials established back in May 2012, almost a year and a half before the roll out of Healthcare.gov.”).

⁸ Letter from the Donna Pignatelli, Director, OSTP Legislative Affairs, to the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology (January 15, 2014) [hereinafter *January 15 Letter*], at 3. At Chairman Smith’s request, OSTP also produced all documents that it had at that point provided to the Committee on Oversight and Government Reform.

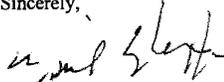
⁹ Email from Steven VanRoekel to J. Michael Daniel, et al. (Apr. 12, 2013, 3:25 p.m.), enclosed.

cybersecurity defenses in place, but instead served as an intermediary and relied on the HHS and CMS officials to provide the substance of the information he then passed on to others.¹⁰

Third, shortly before the first open enrollment period, Mr. Park also served as a liaison with cybersecurity officials at HHS and CMS in connection with efforts to explain publicly the cybersecurity protections for the health insurance marketplaces. This “spokesman” function is one Mr. Park performed from time to time as CTO with respect to technology issues generally. Importantly, the enclosed emails again confirm that Mr. Park was not speaking from direct personal knowledge or experience on cybersecurity—before participating in a press call, he solicited the relevant information from CMS cybersecurity personnel and sought to have them participate in the call given his relative lack of familiarity with cybersecurity issues.¹¹

The information provided in and with this letter is consistent with what OSTP has previously explained: that CMS is best positioned to address the Subcommittee’s questions regarding the security of the website and that Mr. Park has not been substantially involved in developing or managing the “specific security standards and technical measures . . . in place to protect Americans’ privacy and personal information that passes through the Healthcare.gov website” More importantly, if the Subcommittee desires additional information, there is no need to resort to subpoenas. Mr. Park will be pleased to testify at a Subcommittee hearing in November. OSTP is also actively searching for additional records that may further illuminate Mr. Park’s relatively minor role on cybersecurity issues and is willing to voluntarily produce additional documents to aid the Subcommittee’s inquiry. Please simply have your staff communicate the Subcommittee’s priorities in that regard to OSTP.

Sincerely,



W. Neil Eggleston
Counsel to the President

¹⁰ Email from Todd Park to Tony Trenkle, et al. (Sept. 2, 2013, 1:14 p.m.), enclosed (“Hi Tony, many apologies for interrupting your Labor Day, but can you help Chris with his follow-up question below (reference to ‘current federal standards and how they exceed private sector as well as track record of protection from attacks’).”).

¹¹ Email from Todd Park to Tony Trenkle, et al. (Sept. 17, 2013, 9:54 p.m.), enclosed (“I’ve let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can talk to it at a general level only -- she thinks that will be OK on the call tomorrow, with detailed questions to be referred to agencies.”).

cc: The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology

The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Dan Maffei
Ranking Minority Member
Subcommittee on Oversight

HEARING DOCUMENTS SUBMITTED BY MAJORITY STAFF

From: Park, Todd
Sent: Thursday, April 11, 2013 4:58 PM
To: VanRoekel, Steven
Subject: RE: Coordination on ACA

Hey brother, thanks so much for the note and the chat! Many apologies for not staying in tighter sync with you on this will make sure we stay in close sync going forward.

Laura is rescheduling the site visit to happen in the next week or two, and we're going to have our ACA Next Steps meeting tomorrow with our smaller circle of WH folks to discuss the red team results and recommendations further (you'll see how unflinchingly clear-eyed and paranoid the red team was, as red teams need to be!) and also to discuss the path forward on the interagency steering committee (which sounds like it has already evolved into its ideal form going forward).

And then separately, Laura is also setting up more 1 to 1 time for you and me to talk about how we optimally coordinate across our joint portfolio. As a hint of coming attractions, you're going to need to stay involved in ACA ☺

It is absolutely awesome to be your teammate, and I truly treasure the incredible collaboration -for-the-public-good we've forged across our offices, which I really do think of as a single team. May the double helix of awesomeness continue, and may the Force continue to be with us ☺

Todd

From: VanRoekel, Steven
Sent: Thursday, April 11, 2013 2:31 PM
To: Park, Todd
Subject: Coordination on ACA

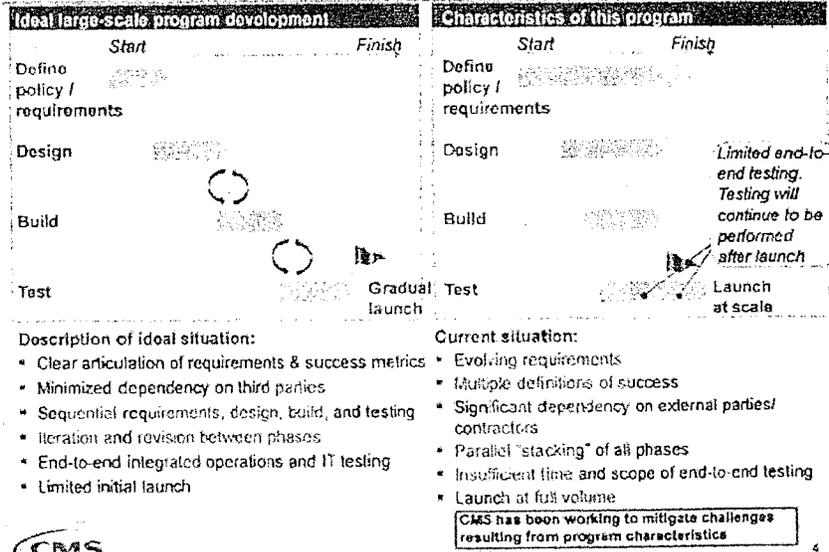
Todd, On ACA - I am hearing some feedback from both inside and outside the building about briefings to the President next week, coordination on a "Red Team" with CMS, suggestions that we cancel the steering committee meeting, suggestion that I not do a CMS visit tomorrow, and more. These raise concerns for me because when it's time to publicly deliver on ACA, I will be the one called to the Hill to testify and, per my statutory authority, will be held accountable for the successful delivery of this project. I anticipate there being increased Congressional scrutiny on the FFE as we move forward. This is just as critical to the legacy of many Congresspeople as it is to the President, and that will raise the likelihood of oversight hearings.

I am not trying to land grab in any way, I just worry that we are uncoordinated here, and that given your history and closeness with HHS, you are not hearing what I am hearing from the budget people in OMB, other agencies (other than CMS) and the private sector that CMS is not being inclusive and is not leading a coordinated effort that will lead to success. I am also worried that you getting a too-CMS-centric picture.

I would love nothing more than this not to be the case, to be assured ACA implementation is on a path we want it to be on, and that existing efforts will deliver what we want.

I think we should, as our next meeting on ACA, sit down, without staff, and have a 1:1 to talk about how we coordinate going forward.

Programs of this type ideally have a sequential planning, design, and implementation process with significant testing and revision



Confidential and Proprietary — Pre-decisional information

Centers for Medicare & Medicaid Services

[REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Friday, August 23, 2013 11:18 AM
To: Chao, Henry (CMS/OIS)
Cc: Mielke, Dawn M.; Graubard, Vivian
Subject: Calling Red Hat

Hey brother, great to speak with you this morning – just wanted to let you know that I could be available to call Red Hat at 1 pm or between 3 to 4 pm.... Might that work for you? I get on a flight at 5 pm – but can totally delay that if needed.... Just let me know, thanks!

Todd

To: Couts, Todd (CMS/OIS) ([redacted])
Cc: Calem, Mark (CGI Federal) ([redacted]); Weiss, Paul (CGI Federal) ([redacted])
From: Manambedu, Lakshmi (CGI Federal)
Sent: Fri 7/12/2013 6:11:47 PM
Subject: RE: Need a write up for Todd
[Day One Capabilities - Priority and Risk - 20130712.docx](#)

Hi Todd,

Attached is what I have for E&E. You may be able to extract the major ones from this.

In terms of other major milestones between Oct 1 and Jan 2014 are:

- Enrollment Reconciliation -- December 2013
- Exemptions Applications -- December 2013
- Payment to Issuers -- 3rd week of January 2014

Thank you

Lakshmi Manambedu | Vice President, CGI Federal | Mobile: ([redacted]) | www.cgi.com

From: Chao, Henry (CMS/OIS) [mailto:henry.chao@([redacted])]
Sent: Friday, July 12, 2013 12:58 PM
To: Manambedu, Lakshmi (CGI Federal); Kariton Kim (kkim@([redacted])); Donohoe, Paul X. (CMS/OIS); Couts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Cc: Oh, Mark U. (CMS/OIS); Berkley, Katrina (CMS/OIS); Couts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: Need a write up for Todd
Importance: High

This is for sources material for Todd Park to pick nuggets from in his prep for briefing POTUS next week.

So the write-up which are sentence(s) in bullet format needs to cover:

- [REDACTED] The A-Z of testing by partner (Issuer, # of Issuers, State programs, types of Marketplace, approach (waves, fairness, DE, 834/enrollment, etc.), and high level schedule.
- [REDACTED] Overall list of key activities to be accomplished and risks for Day one (remaining 80 days) and Day ones for other major lifts prior to Day one of the benefit and the start of the benefit.

Please use material we have already like the deck that we used for SVR and updated another version for Marilyn/OL a few days ago.

Remember that bullets should not be written to be used to create more questions.

Rhonda and Todd—please collect, format, and send to me by COB today.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services

[REDACTED]
[REDACTED]

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Sunday, September 29, 2013 6:22 PM
To: Park, Todd
Subject: Re: Discussion points

Just so you know she decided in January we were going no matter what - hence the really cruel and uncaring march that has occurred since January when she threatened me with a demotion or forced retirement if I didn't take this on - do you really think she has enough understanding of the risks to fight for a delay - no and hell no - for just one moment let's be honest with each other. I appreciate you belief in the goodness of others but at this point I am too tired to pretend there is a decision to be made - it is just how much crap my team will have to take if it isn't sufficiently successful - you haven't lived through the temper tantrums and threats for the last 9 months.

OK - that felt good - - am now back to my role as no comment civil servant

Delete this after reading - promise

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 05:54 PM
To: Snyder, Michelle (CMS/OA)
Subject: RE: Discussion points

Yes, got it. On the call with MT, Chris, and Jeanne, MT said that she appreciates the additional info we will generate tonight, but that she and she alone will make the decision to go or not - which of course is right. And the way she is thinking about it from a performance standpoint is that if enough of the additional hardware gets online to give us an insurance policy, she is comfortable proceeding, with 90,000 concurrent users being far beyond the 50,000 that was the CMS target.

Because new hardware is going live on a rolling basis today and tomorrow, I think we are in very good shape on the hardware front - and because the Miami equipment got here so early today, we've got a good shot at that being live and helping us get to 90,000.

Will be good tonight as per one of the questions for the 9 pm to get people's guesstimate of what kind of traffic in general (order of magnitude) would be associated with a 90,000 concurrent user scenario, just so MT has that.

And will also be good to understand the EIDM situation a bit better to see if that is a separate bottleneck with a lower concurrent user threshold? And if that's a possible threat to monitor. Again, just to inform MT.

Going to deliver cupcakes now :)

----- Original Message -----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]

Because new hardware is going live on a rolling basis today and tomorrow, I think we are in very good shape on the hardware front – and because the Miami equipment got here so early today, we've got a good shot at that being live and helping us get to 90,000.

Will be good tonight as per one of the questions for the 9 pm to get people's guesstimate of what kind of traffic in general (order of magnitude) would be associated with a 90,000 concurrent user scenario, just so MT has that.

And will also be good to understand the EIDM situation a bit better to see if that is a separate bottleneck with a lower concurrent user threshold? And if that's a possible threat to monitor. Again, just to inform MT.

Going to deliver cupcakes now :)

-----Original Message-----

From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]
Sent: Sunday, September 29, 2013 4:02 PM
To: Park, Todd
Subject: Re: Discussion points

These are helpful but we are going live one way or another. MT has made it clear to me that that question isn't on the table. It is more knowing how to message what won't work

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto: [REDACTED]]
Sent: Sunday, September 29, 2013 02:42 PM
To: Snyder, Michelle (CMS/OA)
Subject: Fw: Discussion points

Hi M, just sending this to you so I don't distract folks in mid-flight this afternoon. On load/performance, it will be very helpful at the end of the day for you to do a gutcheck -- with Henry and Dave and whomever else they'd like to include (I'm happy to join as well) -- to net out where we are, make an educated guess about what is likely to happen on Oct 1, and recommend to Marilyn that we go/no go. I'm sure you have already thought this through, but here's a sample "logic path" to talk through with Henry/Dave and team, building on the questions from the earlier email (I know you're hyperfocused on other items like call center right now, so I thought I might prep this for you at least as a draft):

-- Does the performance testing that the team has done give you confidence that the FFM can handle 21,000 concurrent users with existing hardware and about 90,000 concurrent users with the new hardware added -- with great user response times? What might the holes be in terms of our knowledge of system performance?

-- Where are we in the installation and activation of the new hardware? How confident are we that all of it will be online and ready by Monday COB?

-- Confirm that the 90,000 concurrent user figure means that literally 90,000 people can be hitting the exact same keystrokes, doing the exact same thing, stressing out the exact same precise part of the FFM, at the exact same time

– Confirm that what for sure doesn't impact the FFM's functionality or access is if there happens to be a zillion of her people hitting the homepage/"Learn about the Marketplace" pages on HealthCare.gov at that same moment, because it's technically separate from the Get Insured workflow. (And you should confirm that the homepage/"Learn" pages on HC.gov are ready for an onslaught (including Akamai caching))

– Question: while 90,000 users in the FFM functionality itself are all doing the exact same thing to the FFM in a single unified punch at the same millisecond, what can other users in the FFM workflow be doing? Can many others be "in between" clicks i.e., reading a page, filling out fields on a webpage before hitting submit, surveying their plan options? What is our even rough intuitive sense about if others can also be actively exercising different parts of the FFM different clicks on different functionality?

– Based on the above and what we might guesstimate about Day 1 use patterns, what kind of overall total FFM user volume for Day 1 do we think is supportable if we can support 90,000 concurrent FFM workflow users? (This is obviously going to be a swag, because it's hard to predict distribution of visits over the course of the day, but Dave/Henry may have some instincts about this based on past experience)

– What happens after the 90,000 concurrent user threshold is reached? Is there gradual degradation of response time for users? Rapid degradation? Immediate crashing?

– What is your best professional gut guess (based both on what you know and don't know) as to the percentage probability that the system will slow to unacceptable levels of performance, or crash entirely? (They may only really be able to give you a qualitative sense of this)

– Should we go live on Oct 1?

Again, just a suggestion/draft as to the logic path – feel free to shred/add items/delete items/change entirely :)

----- Original Message -----

From: Park, Todd

Sent: Sunday, September 29, 2013 10:27 AM

To: Snyder, Michelle (CMS/OA) <[REDACTED]>; Chao, Henry (CMS/OIS) <[REDACTED]>;

Bowen, Marianne (CMS/OA) <[REDACTED]>

Subject: RE: Discussion points

Hi Michelle, as your consigliere, I do recommend that you ask the questions below – which are of course questions that Henry is already asking himself, but it would be good for you to know the answers as well :)

And Henry, needless to say: work to actually continually make key things better takes absolute precedence over question answering :)

And again, the only questions you should answer are from Michelle :) I've added her additional question and put it at the top of the recapped list below (and have also adjusted the numbers based on the update). She can pick from #2 through #6 below and designate which ones she really cares about :)

And I've taken a shot at answering some of them (#2, #4, #5) based on my understanding from the brief discussion this morning – which Henry can correct as necessary:

(1) Would it help to have someone like NGS help with the testing on an ongoing basis?

A:

From: Park, Todd
Sent: Sunday, September 29, 2013 7:13 PM
To: 'Michelle.Snyder [REDACTED]'
Subject: Re: Discussion points

M, I think (knock on wood!!!!!!) that you and team are actually going to pull off the feat of the century -- a feat that will go down in history, and literally change the course of history for the better. No other team could have possibly come close to what you've done and are doing. No one.

We all as Americans owe you and team an extraordinary debt of gratitude -- for your incredible ingenuity, your deep sacrifice, your superhuman level of effort and focus, your extraordinary tenacity. You have my word that I will continue to do everything in my power to make sure everyone understands this in the months and years ahead. I know y'all are not chest-thumpers -- that's part of what I love about all of you -- but I really do think that it's important for folks to understand how absolutely incredible you and team are, and I will continue to spread that understanding.

Please don't ever hesitate to ask me for anything I can do to be helpful on this or any other front -- and if there is any way for me to help celebrate the team -- whether it be cupcakes :) or a meeting with POTUS (which I will start working on)

Semper fi, and much love,
Todd

----- Original Message -----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 07:03 PM
To: Park, Todd
Subject: Re: Discussion points

And I have kept this all from my team. Marianne and Jim and Andi know about how bad it has been. The rest need the illusion - the four of us have none left

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 05:54 PM
To: Snyder, Michelle (CMS/OA)
Subject: RE: Discussion points

Yes, got it. On the call with MT, Chris, and Jeanne, MT said that she appreciates the additional info we will generate tonight, but that she and she alone will make the decision to go or not -- which of course is right. And the way she is thinking about it from a performance standpoint is that if enough of the additional hardware gets online to give us an insurance policy, she is comfortable proceeding, with 90,000 concurrent users being far beyond the 50,000 that was the CMS target.

Message

From: Tavenner, Marilyn (CMS/OA) [/O=HHS EES/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MARILYN.TAVENNER.CMS]
Sent: 6/26/2013 9:55:47 PM
To: "Todd_Y_Park [mailto: [REDACTED]]"; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.OS]
CC: Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana_Khalid.CMS]
Subject: Re: Follow-up

Thanks Todd. Appreciate the help as always!!!!

From: Park, Todd [mailto: [REDACTED]]
Sent: Wednesday, June 26, 2013 05:34 PM
To: Tavenner, Marilyn (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Follow-up

Hi Marilyn, Michelle, and Henry,

After talking with Henry and team, I spoke with Mark about the logo issue, and explained why attempting to add logos for October 1 is extremely unwise. He understands. He may want me to get on the phone with someone from the Blues so they fully understand it. I'm more than happy to do so on your behalf – this issue should not consume any more of your time.

Marilyn, I'm also going to visit with Henry and team for one of our evening deep-dive sessions to get up to speed on the latest status of IT and testing – during the week of July 8. Michelle, Henry, and I had a check-in call today, but I think that Henry is right that to really understand current status and next steps, there is no substitute for an evening deep-dive. So I'll bring healthy food and snacks to Baltimore and camp out with Henry and team for a few hours ☺

All the best,
Todd

Both Julian and David took great pains to ask that the visit not be disruptive to your work -- I think that the message to give y'all the space to rock and roll is spreading :)

So I'm thinking a focused two-hour visit, in Baltimore, going thru the live workflow, and using high-level materials you already have.

Would next week be best, or would the week after be better, or would either week be fine? I haven't yet pinged David and Julian for their availability, but wanted to see what was optimal for you first. It would be good to combine both of their visits, to save you time. Thoughts on timing?

Michelle, it would be terrific for you to join -- would be great for you to meet Julian and David, both of whom are terrific; and I've told both of them that you and Henry are pure awesomeness :)

Thanks!
Todd

----- Original Message -----

From: Chao, Henry (CMS/OIS) [redacted]
Sent: Thursday, July 25, 2013 09:53 AM
To: Park, Todd
Cc: Oh, Mark U. (CMS/OIS) [redacted]; Coutts, Todd (CMS/OIS)
[redacted]; Outerbridge, Monique (CMS/OIS)
[redacted]; Grothe, Kirk A. (CMS/OIS)
[redacted]; Berkley, Katrina (CMS/OIS)
[redacted]; Rhones, Rhonda D. (CMS/OIS)
[redacted]; Graubard, Vivian;
[redacted]; <rich.martin@hhs.gov>;
<cheryl.campbell@hhs.gov>;
<Lakshmi.Manambedi@hhs.gov>;
<Mark.Calem@hhs.gov>; Wallace, Mary H.
<Paul.Weiss@hhs.gov>; Booth, Jon G. (CMS/OC)
(CMS/OC) [redacted]

Subject: Walk through of the online application in hc.gov

Todd,

If you recall we had agreed to provide you a walk through and demo of the online application in its current form so you can get a chance to peek under the covers of hc.gov.

Key Points Discussed		
No.	Topic	Highlights
2	Workgroup Updates	<p>dependencies from consent.</p> <p>Marilyn Tavenner has been engaged in the consent resolution conversations.</p> <ul style="list-style-type: none"> • Details cannot be flushed out until these conversations are complete. • CMS has been ordered to await the completion of these discussions before determining the necessary changes to the baseline schedule. <p>Todd Park has been engaged in discussion on NIST Level 2 inter-mechanics.</p> <ul style="list-style-type: none"> • CMS is moving forward with following this process, which represents SSA's understanding, as well. • SSA is interested in understanding the downstream impact on the overall integrated testing, as well as the timeline. <p>Scheduling</p> <ul style="list-style-type: none"> • Highest risk to implementation associated with awaiting the high-level decision, as opposed to building for the worst case scenario. <ul style="list-style-type: none"> ◦ Broad risk: Schedule and implementation risks would be the largest concerns. The schedule presents a risk of a 2-4 week delay. ◦ The team must agree that the schedule risk is a priority and must find ways to retrieve the lost time from other areas. ◦ It is unclear as to whom the secretary is in discussion with or what the status of the discussion is. ◦ Teams thought there would be simultaneous development between the legal issue and the IT build as the higher level issues were being addressed. The interagency team is not in full agreement on this issue. ◦ David Black would like the teams to continue making technology progress. <p>Clarification: Identification Proofing vs. Consent</p> <ul style="list-style-type: none"> • Consent is a legal issue, whereas, identity proofing is a solution and process that needs to be established. • SSA is relying on the Privacy Act for legal authority on ID proofing as there is none provided in the Act. <ul style="list-style-type: none"> ◦ Legal team is currently working this issue. ◦ Identity proofing would be built in as a process for verifying an individual's identity. • Previous decision to use two IRS challenge questions at the threshold has been reconsidered and is currently being discussed. • Suggestion: A smaller group of key individuals may need to reconvene on this topic in 3-4 weeks including Marilyn because of her involvement with the scheduling. <p>Integrated Project Plan</p> <ul style="list-style-type: none"> • The IPP needs to be addressed before focusing on the schedule

From: Fasching, Laura <[REDACTED]>
Sent: Saturday, September 28, 2013 10:47 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Glad to help, let me know if you need anything else gentlemen ☺
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 10:38 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

That is super-awesome Laura, thanks so very, very, very much!!!!

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 10:36 PM
To: Chao, Henry (CMS/OIS); Park, Todd
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd & Henry,

The shipper is picking up the equipment in the next 90 minutes from the Miami data center and we expect the shipment to arrive between 9:30 AM to 10:00 AM. ☺

So Monday COB is looking good as long as we keep the shippers on schedule, as the build teams will be working at 6 am with the equipment that was brought in today.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 9:03 PM
To: Fasching, Laura; Todd Y Park [REDACTED]
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

I got the approval from our COO and head of Contracts to go with the 40k option.

Contracts said we will have to work out how this can be a line you can bill in the contract but no problem figuring that out later.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

(Pri)
(Alt)
(BB)

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 09:00 PM
To: Park, Todd < >; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura < >
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Ok great Henry can I get confirmation that the Government will pay for the plane? We have to get David Small's Approval so we will need to call him as soon as possible.

Thanks and sorry to rush you all.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel:
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:]
Sent: Saturday, September 28, 2013 8:50 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

FYI, the private plane option I am pursuing would likely cost about the same as the Fedex expedite cargo plane option below.

Henry, I think that delivery to the data center mid-day Sunday sounds really, really, really good...

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 8:46 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?
Importance: High

Ok here is what I was able to do
I was able to get to FedEx custom Critical they can drive it to us via a truck with pick up tonight @ 11:00 PM (ish) and delivery around 9 PM on Sunday night for \$3700.00
Or

To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Laura, by when do you need to make a decision about whether to send via private ground, private cargo plane, or Air Force (if Air Force is indeed an option?)

And to confirm private ground would deliver the hardware on Tuesday (to be installed Wednesday?), private cargo plane would deliver the hardware on Monday (to be installed Tuesday?). With no possibility of acceleration of those timetables?

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 7:29 PM
To: 'laura.fasching [REDACTED]'; Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd--it's in your hands now to make a quick decision.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Fasching, Laura [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 07:27 PM
To: Park, Todd < [REDACTED] >; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

We have been exploring that option too but no luck so far

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 7:26 PM
To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Also: as another option to explore, in the interest of exploring all options simultaneously, is it possible to arrange for heroic chartered private sector ground transportation that could get going super-early tomorrow morning and get to Culpeper by Sunday evening?

From: Park, Todd
Sent: Saturday, September 28, 2013 7:03 PM

To: 'Chao, Henry (CMS/OIS)'; 'laura.fasching [REDACTED]'
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

WH team responded instantly, is working on it as we speak and will get back to us ASAP. But they unfortunately are not optimistic, so we should explore other options in parallel.

Is there any possibility of arranging for private/commercial cargo plane transport? Chartered, even?

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 6:35 PM
To: 'laura.fasching [REDACTED]'
Cc: Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Just talked to Todd and he is going to talk to the rest of WH that can make this happen so just reply with the confirmed service to Homestead.

Todd--let us know ASAP so laura will send via ground if you can't arrange for transport to someplace the Air Force can land near Culpeper VA.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 06:09 PM
To: Chao, Henry (CMS/OIS)
Cc: Fasching, Laura <[REDACTED]>
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Henry,

We are working on firming up the white glove shippers but once that is done we would be good to go.

If we get the shippers scheduled and the equipment gets here tomorrow my engineers said they have the resources to build it out and just like we said before up by cob Monday.

I will let you know about the shippers within an hour.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Fasching, Laura <[REDACTED]>
Sent: Tuesday, October 01, 2013 2:08 AM
To: Park, Todd; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thuiston, Robert (CMS/CTR); Fasching, Laura
Subject: RE: New expansion

Todd & Henry

As we have been working with your team to assist you in making the Marketplace launch successful, we continue to work to adapt to your needs.

Right now, I understand that while we add more compute, the team needs the VMs built faster.

In this tasking we are using the best practices that were agreed to as to not induce risk into your builds

- such as utilizing the kickstart process (custom templates of the hardened images) for RHEL 5 & 6; Windows VMs the SQL VMs utilizes a standard image which requires additional time to harden to NIST standards.

However we have found that due to the size of this environment 1500 + VMs, we are seeing an impact to running too many builds at once. As doing too builds at once slows down the process by overwhelming the Virtual Center server.

The options we have to increase the speed of the VM builds introduce a **SIGNIFICANT RISK** to the environment. We do not suggest either of these options, but I wanted to give you a full picture of the situation.

1. VC Client Basically cloning of existing VMs and while this may seem an easy option
 - a. Old network configs and FW rules have to be removed first. Then the new ones need to be done. very time consuming and manual
 - b. Finally, these VMs will not appear in iCenter. Without them being visible in iCenter, these VMs will be unmanageable in the future & you will not be able to manage the compute resources.
2. VM import may get the VM's in place but they have the exact same issues as noted above.

We have engaged our vendor URS to increase staffing during this time, and will follow up shortly on the results of that endeavor. If we can get a couple more people in now it will assist with allowing some team members to focus on the builds while other field calls and assist with troubleshooting.

Just as we did yesterday when we receive an request for more storage resources than were in either the reserve capacity or in the expansion order. We will work to adapt to your needs during as you bring the Affordable Care Act's Insurance Exchanges to the American public.

Thanks
 Laura

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: [REDACTED]
 222 W Las Colinas Blvd, Irving, Texas, 75039



DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

 Administrator
 Washington, DC 20201

SEP 10 2013

The Honorable Bennie Thompson
 Ranking Member
 Committee on Homeland Security
 U.S. House of Representatives
 Washington, DC 20515

Dear Representative Thompson:

Thank you for your inquiry related to privacy and security protections associated with the Data Services Hub (Hub) and the status of our work to protect people and programs from cyber-attacks in this area. At the Department of Health and Human Services (HHS), we take very seriously our responsibility to safeguard personal information in all of our programs, including in the Affordable Care Act Marketplace. Collectively, the tools, methods, policies, and procedures we have developed provide a safe and sound security framework to safeguard consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage starting on October 1, 2013. This framework is consistent with the framework that exists for all other HHS programs, such as Medicare, which Americans rely on every day.

HHS's Centers for Medicare & Medicaid Services (CMS) has a strong track record of preventing breaches involving the loss of personally identifiable information from cyber-attacks. This is due in large part to the establishment of an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. Our system and security protocols are grounded in statutes, guidelines and industry standards that ensure the security, privacy, and integrity of our systems and the data that flow through them. These protections include a series of statutes and amendments to these laws, such as the Privacy Act of 1974, the Computer Security Act of 1987 and the Federal Information Security Management Act (FISMA) of 2002, as well as various regulations and policies promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology (NIST).

In accordance with these provisions, CMS has developed the Hub, a routing tool that helps Marketplaces provide accurate and timely eligibility determinations. **It is important to point out that the Hub will not retain or store Personally Identifiable Information.** Rather, the Hub is a routing system that CMS is using to verify data against information contained in already existing, secure and trusted federal and state databases. CMS will have security and privacy agreements with all federal agencies and states with which we are validating data. These include the Social Security Administration, the Internal Revenue Service, the Department of Homeland Security, the Department of Veterans Affairs, Medicare, TRICARE, the Peace Corps and the Office of Personnel Management.

The Hub is designed to comply with the comprehensive information security standards developed by NIST in support of FISMA. NIST has emerged as the gold standard

Page 2 - The Honorable Bennie Thompson

for information security standards and guidelines that all federal agencies follow. Several layers of protection will be in place to help protect against potential damage from attackers and mitigate risks. For example, the Hub will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action against irregular behavior and unauthorized system changes that could indicate potential attacks. Automated methods will ensure that system administrators have access to only the parts of the system that are necessary to perform their jobs. These protocols, combined with continuous monitoring, will alert system security personnel when any system administrator attempts to perform functions or access data for which they are not authorized or are inconsistent with their job functions.

Should security incidents occur, an Incident Response capability built on the model developed by NIST would be activated. The Incident Response function allows for the tracking, investigation, and reporting of incidents so that HHS may quickly identify security incidents and ensure that the relevant law enforcement authorities, such as the HHS Office of Inspector General Cyber Crimes Unit, are notified for purposes of possible criminal investigation.

Before Marketplace systems are allowed to operate and begin serving consumers across the country, they must comply with the rigorous standards that we apply to all federal operational systems and CMS's Chief Information Officer must authorize the systems to begin operation. I am pleased to report that the Hub completed its independent Security Controls Assessment on August 23, 2013 and was authorized to operate on September 6, 2013. The completion of this testing confirms that the Hub complies with the stringent standards discussed above and that HHS has implemented the appropriate procedures and safeguards necessary for the Hub to operate securely on October 1.

The privacy and security of consumer data are a top priority for HHS and our federal, state, and private partners. We understand that our responsibility to safeguard our systems is an ongoing process, and that we must remain vigilant throughout their operations to anticipate and protect against evolving data security threats. Accordingly, we have implemented privacy and security measures for the Marketplace systems that employ measures similar to those in the private sector and we will continually validate through a variety of methods.

In closing, we have produced an extremely strong enterprise information security program by implementing state-of-the-art controls and business processes based on statutory requirements, agency and organizational commitments, best practices, and the experience and knowledge of our subject matter team members. This has resulted in the development, testing and readiness of the Hub to operate on October 1 to serve consumers across the country in a secure and efficient manner. We hope this information is responsive to your inquiry. Thank you for your interest in and leadership on this important issue.

Sincerely,



Marilyn Tavenner

From: Russell, DeLaine <[REDACTED]>
Sent: Wednesday, September 11, 2013 11:10 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Park, Todd; Cook, Brian T. (CMS/OC); Aronson, Lauren (CMS/OL); Snyder, Michelle (CMS/OA); Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Gartner

Tony,
 Thank you for sending the letter. I have identified Gartner analyst Christian Byrnes, who will review and provide comment. Christian is a managing vice president at Gartner. His team is distributed across the globe and covers the management of risk-related programs such as Information Security, Business Continuity, Privacy and Compliance. In addition, he confers with leading organizations worldwide on technology direction, security trends and best practices. I will provide his response as soon as possible.

DeLaine

DeLaine Russell | Vice President - Public Sector | Gartner, Inc. | 4501 N. Fairfax Dr. | Arlington, VA 22203 | U.S.A. |
 Office: +[REDACTED] | Fax: +[REDACTED] | Mobile: +1 [REDACTED] | Email: [REDACTED] |
www.gartner.com

P Please consider our environment before printing

-----Original Message-----

From: Trenkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, September 11, 2013 11:00 AM
To: Russell, DeLaine
Cc: Park, Todd; Cook, Brian T. (CMS/OC); Aronson, Lauren (CMS/OL); Snyder, Michelle (CMS/OA); Baitman, Frank (OS/ASA/OCIO); Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: FW: Gartner

Hi DeLaine,

Per our conversation here is the letter that went to the Committee. Please let us know what your analysts' thoughts are.

Thanks.

Tony

>-----Original Message-----

>From: Aronson, Lauren (CMS/OL)
 >Sent: Wednesday, September 11, 2013 9:12 AM
 >To: Park, Todd; Trenkle, Tony (CMS/OIS)
 >Cc: Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
 >Subject: RE: Gartner
 >
 >Here's the final signed letter.

From: Trenkle, Tony (CMS/OIS) [mailto: [REDACTED]]
Sent: Thursday, September 12, 2013 08:49 AM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) < [REDACTED] >; Fryer, Teresa M. (CMS/OIS) < [REDACTED] >; Mellor, Michael (CMS/OIS) < [REDACTED] >
Subject: FW: Comment from Gartner Analyst Christian Byrnes

Todd,

Does this help?

Tony

From: Russell, DeLaine [mailto: [REDACTED]]
Sent: Wednesday, September 11, 2013 12:04 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Heiliger, Christopher
Subject: Comment from Gartner Analyst Christian Byrnes

Tony,

Below is what I just received from the analyst. I hope this is what you are looking for. Chris is our most knowledgeable and experienced information security analyst.

Best,
DeLaine

Gartner Inc advises thousands of enterprise and government clients on best practices associated with the use of information technology. As a leader of the information security practice within Gartner Research I certify that the statements made in this letter represent current best practices for the protection of sensitive and regulated data and systems.

F. Christian Byrnes
Managing Vice President, Risk and Security Program Management
Gartner Inc.
[REDACTED]

DeLaine Russell | Vice President - Public Sector | Gartner, Inc. | 4501 N. Fairfax Dr. | Arlington, VA 22203 | U.S.A. | Office: + [REDACTED] | Fax: + [REDACTED] | Mobile: +1 [REDACTED] | Email: [REDACTED] | www.gartner.com

 Please consider our environment before printing

This e-mail message, including any attachments, is for the sole use of the person to whom it has been sent, and may contain information that is confidential or legally protected. If you are not the intended recipient or have received this message in error, you are not authorized to copy, distribute, or otherwise use this message or its attachments. Please notify the sender immediately by return e-mail and permanently delete this message and any attachments. Gartner makes no warranty that this e-mail is error or virus free.

From: Aronson, Lauren (CMS/OL) <[REDACTED]>
Sent: Thursday, September 12, 2013 10:14 AM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS); Cook, Brian T. (CMS/OC)
Subject: RE: Comment from Gartner Analyst Christian Byrnes

Yup. We have Gary Cohen testifying before Energy & Commerce next week so we could potentially use this.

From: Park, Todd [mailto:[REDACTED]]
Sent: Thursday, September 12, 2013 10:13 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS); Cook, Brian T. (CMS/OC); Aronson, Lauren (CMS/OL)
Subject: Re: Comment from Gartner Analyst Christian Byrnes

Tony, I think this is super-helpful – Brian and Lauren, perhaps this is something you can hold in reserve in case you need it?

From: Trenkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Thursday, September 12, 2013 08:49 AM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) <[REDACTED]>; Fryer, Teresa M. (CMS/OIS) <[REDACTED]>; Mellor, Michael (CMS/OIS) <[REDACTED]>
Subject: FW: Comment from Gartner Analyst Christian Byrnes

Todd,

Does this help?

Tony

From: Russell, DeLaine [mailto:[REDACTED]]
Sent: Wednesday, September 11, 2013 12:04 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Helliger, Christopher
Subject: Comment from Gartner Analyst Christian Byrnes

Tony,
Below is what I just received from the analyst. I hope this is what you are looking for. Chris is our most knowledgeable and experienced information security analyst.
Best,
DeLaine

Gartner Inc advises thousands of enterprise and government clients on best practices associated with the use of information technology. As a leader of the information security practice within Gartner Research I certify that the

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Thursday, October 10, 2013 5:03 PM
To: Park, Todd
Subject: FW: Item

A. Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

From: Trenkle, Tony (CMS/OIS)
Sent: Thursday, October 10, 2013 4:54 PM
To: Snyder, Michelle (CMS/OA); Tavenner, Marilyn (CMS/OA); Kerr, James T. (CMS/CMHPO)
Subject: RE: Item

Here's the answer below, maybe more detail than you want.

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, October 10, 2013 2:08 PM
To: Fryer, Teresa M. (CMS/OIS)
Cc: Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS)
Subject: RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

Statement:

CMS (CIISG) acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the java script posted on-line. The code base at CGI has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The XOC Security team and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform JS comment-removal/minification/obfuscation is a roadmap item, in fact it is scheduled for release to the Test2 environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during YUI compression. As java scripts can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a

consumer as A Good Consumer Experience was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP
Information Security Officer, CCIIO
CMS\OIS\CIISG
Consumer Information and Insurance Systems Group
[REDACTED] (Balt. Office, N2-13-22)
[REDACTED] (Mobile)

From: Snyder, Michelle (CMS/OA)
Sent: Thursday, October 10, 2013 4:41 PM
To: Trenkle, Tony (CMS/OIS)
Subject: Fw: Item

Could you take a look?

Sent from my BlackBerry Wireless Device

From: Tavenner, Marilyn (CMS/OA)
Sent: Thursday, October 10, 2013 04:10 PM
To: Snyder, Michelle (CMS/OA); Kerr, James T. (CMS/CMHPO)
Subject: FW: Item

Wanted you to have this in case you want to have tony reach out to them

From: Park, Todd [mailto:[REDACTED]]
Sent: Thursday, October 10, 2013 2:11 PM
To: Tavenner, Marilyn (CMS/OA)
Subject: Item

Marilyn, this got sent to me by someone who says these guys are on the level. I would suggest that the Marketplace IT security folks check it out (and potentially reach out to these guys as well)

https://www.trustedsec.com/october_2013/affordable_health_care_website_secure_probably/

Contact Us: 1.877.550.4728 | info@trustedsec.com



Home Services Downloads Blog About Us Contact Us Q

Is the Affordable Health Care Website Secure? Probably not.

Home / October 2013 / Is the Affordable Health Care Website Secure?

Probably not.

< Previous Next >

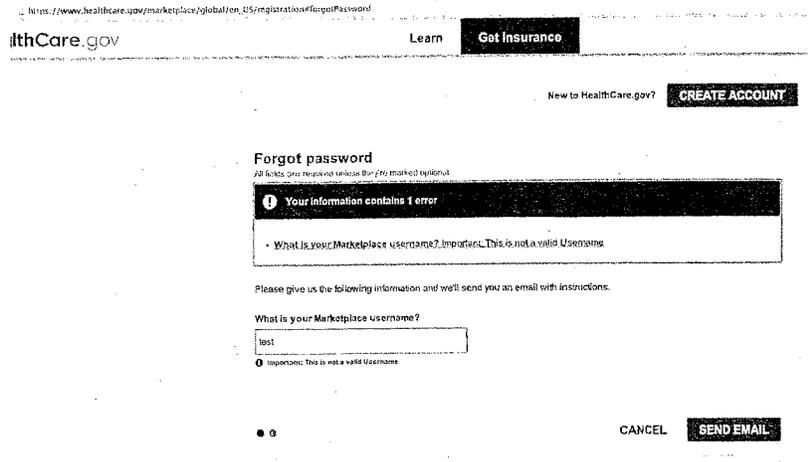
Is the Affordable Health Care Website Secure? Probably not.

With the Affordable Health Care Act moving into full momentum – there are a lot of privacy and security concerns for any new major government program being implemented. It's no secret that the website, the infrastructure, and the staffing has been a challenge to get up in running in the appropriate timeframes. Coming purely from the security industry and seeing corporations, deadlines, and tight timeframes snag security objectives – there should be major concern on the implications this system has on what will become the largest database of Americans in recorded history.

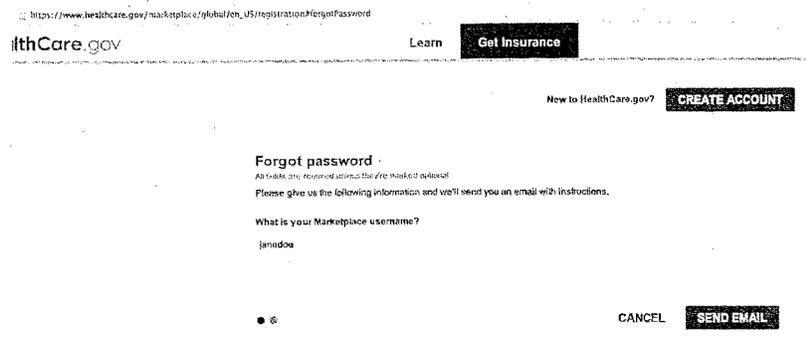
The Affordable Health Care Act websites cost an estimated 634 million to develop. <http://www.digitaltrends.com/opinion/obamacare-healthcare-gov-website-cost/>. One would hope that there would be heavy security integration into the software development lifecycle and best practices followed in the most extreme circumstances. As you can imagine, the site is going to be a major target for hackers, other governments, and organized crime. There's a lot of money to be made right now in an untapped market that is fresh for the picking.

We decided to look around – please note that there was nothing malicious, no hacking, and nothing intrusive involved in this test in any regard. We simply browsed the website as a normal visitor without any type of attacks at all. Just by looking at information, you can determine the quality of the code, and whether simple best practices in security are being followed.

Below is in the "Log In" page and the "Forgot password" link. Note when you enter a username that is invalid, it returns quickly that the username is invalid.



Note when you place a valid user:



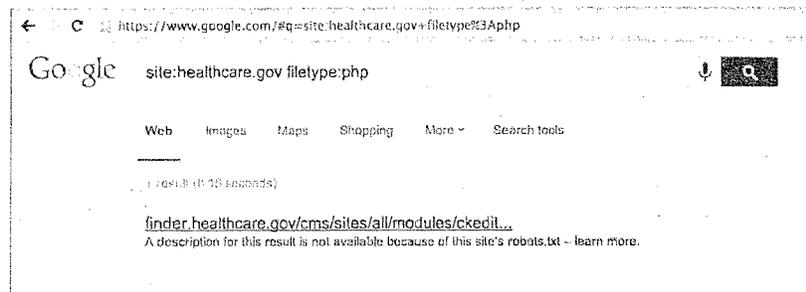
As you can see, you can enumerate valid and invalid user accounts in the database. Even worse is there are no form or appearance of automation deterrents such as CAPTCHA or image verifications that a human is attempting this. We can easily feed this through Burp Intruder for the content length from the response to see which usernames were

actually valid. Essentially you could enumerate the entire database of user accounts in the new healthcare.gov website through brute forcing the response codes and finding valid usernames.

Additionally, developer comment code is plastered everywhere which gives an attacker a significant amount of understanding about the application – these are literally everywhere on almost every page that's opened and all third party files:

```
//global variable used for SHOP upload functionality
var myView = null;
var agentBrokerSAMLToken=null;
var postCCRApplicantIDToken=null;
var postCCRAppIDToken=null;
var postCCRState=null;
var agentEmailUUID =null;
```

Even crazier, doing some Google reconnaissance, we found an indexed site that a subsite used CKEditor – NOTE we did NOT attempt to even follow the link to verify if it's there.



CKEditor has a number of known exposures here: Search results for CKEditor on Exploit-DB

We've also identified some significant ones that we can't post online due to the critical nature of them and attempting to contact the development team for the website to remediate. Our intent is not to point out flaws, show flaws, or demonstrate insecurities, only to bring the light that based on viewing like a normal user, there appears to be things that would indicate that there should be major reason for concern here.

Again – nothing malicious performed here and we truly have no idea what the real exposures are without performing a full test on this, which we would have hoped would have been performed prior to any major production release.

By davek | October 9th, 2013 | October 2013 | Comments Off

Message

From: Park, Todd [REDACTED]
Sent: 6/26/2013 2:03:17 AM
To: Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS];
 Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.OS]
Subject: RE: Draft writeup

Is it possible to get any edits/corrections/additional detail by COB Thursday?

Would love to loop back with Jeanne and Mark on Friday before I head out for (an attempted) vacation from July 1 to July 5. I gave Jeanne a heads up today to telegraph what's coming.

I think that the key will be to give Jeanne and Mark a bulletproof set of talking points they can use to push back in their conversations with the Blues and have the Blues truly understand why the logo play is a bad idea right now. (I don't think the Blues really understand that yet).

From: Snyder, Michelle (CMS/OA) [REDACTED]
Sent: Tuesday, June 25, 2013 5:48 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Subject: RE: Draft writeup

Looks good.....

A. Michelle Snyder
 Deputy Chief Operating Officer
 DHHS/CMS
 [REDACTED]

From: Park, Todd [REDACTED]
Sent: Tuesday, June 25, 2013 1:13 AM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Draft writeup

Please keep close hold – loop in folks who can help with the details, but don't circulate broadly yet, if you don't mind. Let me know if this sounds right – any corrections/edits/additions/deletions welcome:

Attempting to integrate logos into the FFM for October 1 is not advisable. This is not because the act of integrating a logo is by itself a difficult thing to do. It's because the process for collecting health plan and product data from carriers via templates, loading these data into the HIOS system, validating the data, transferring the data from HIOS into the FFM QHP database, and having the rating engine retrieve and render that data in the FFM has been locked down, and is being utilized to support plan data collection/validation and system testing as we speak. Changing the underlying plan data template and processing routine right now -- by adding a new plan data element, the logo -- during the crunch-time sprint we're in from now to October 1, would introduce significant risk. Think of it as trying to change a gear in an airplane engine in mid-flight. Or adding a new field to an IRS tax form in the middle of filing season. As an isolated act, adding the field isn't hard. What's hard is the notion of adding it to the tax form via a system modification when that

system is going through an intense time, with a lot of moving parts involved, and where a wrong move could actually screw the whole system up.

An alternative to changing the core plan data submission/management process and systems (i.e., modifying the carrier plan data templates, HIOS, the QHP database, and rating engine logic) would be to set up a database of logos outside this core data management process and have the FFM system, when rendering a given insurance product, pull from both the QHP database plus the logo database. This is a terrible idea technically, would be prone to error, and still creates the issue of mucking with the jet engine while it's in flight.

The right way to add logos to the FFM would be to modify the core plan data submission/management process and systems to include logos as part of the carrier plan/product template and be able to process logos all the way through. This is not doable for Oct 1 without introducing significant operational risk to the go-live, as discussed above. We suggest considering it as part of a future release, post October 1 – understanding that it will have to compete with a lot of priorities. The reasonable thing to do would be to target making this modification in time for the next cycle of plan bids, in 2014.

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Monday, July 22, 2013 10:45 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Cc: Kerr, James T. (CMS/CMHPO); Bowen, Marianne (CMS/OA); Trenkle, Tony (CMS/OIS)
Subject: RE: BCBSA meeting; chatting tonight
Attachments: Chronological account of testing tasks and current status of Issuer testing 7-22-2013.docx

Importance: High

Please see attached paper that describes where we are currently with testing with issuers and provides a chronology of tasks and attempts to address the issues (most which are not correct or inaccurate) Captured by M. Siegler in a meeting I presume with the BCBSA.

Dan Miller on my staff led the gathering of the facts for this paper and Dan has been what I call the "IT Ombudsman" for CMS and Issuer testing coordination. Dan, myself, and the rest of my staff are willing to do whatever it takes to get the issuers through testing and hope they will work as a community to elevate themselves to an improved operational readiness posture rather than spend time pointing to last month's challenges that have been overtaken by even ts. Their collective energies from Association coordination to marketing to legal to IT to operations should be singularly focused on doing what it takes to get to October 1st.

Thanks and please let me know if you need me to walk you through the descriptions.

Henry Chao
 Deputy CIO & Deputy Director,
 Office of Information Services
 Centers for Medicare & Medicaid Services
 [REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Monday, July 22, 2013 7:33 PM
To: Chao, Henry (CMS/OIS); Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Subject: RE: BCBSA meeting; chatting tonight

Thanks so much, Henry and (echoing Marilyn), take the time you need, and get it to us whenever you can tonight... Thanks so much again,
 Todd

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Monday, July 22, 2013 7:23 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Subject: Re: BCBSA meeting; chatting tonight

We'll address in the write-up coming around 3pm.

Henry Chao

Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

(Pri)
(Alt)
(BB)

From: Park, Todd [mailto:]
Sent: Monday, July 22, 2013 07:16 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: RE: BCBSA meeting; chatting tonight

Hi Henry, just spoke with Marilyn if your writeup tonight could address each point in the Siegler email (including the point about subsidy eligibility and back-end app processing being fully on paper), that would be terrific. For convenience, have repasted the Siegler text below ☺ Thanks so very much again for doing this!

Siegler email: "The specifics I wrote down from the meeting are as follows. BCBS claimed: there was a 90% failure rate on the initial "handshake" tests with issuers and the FFM; as of Friday BCBS had not been able to establish "full connectivity" with the FFM; HHS had scheduled testing of enrollment file transfers to begin on July 15 but that was delayed one week and is set to begin today; BCBS presented HHS with 23 eligibility scenarios (eg: family coverage no subsidy, single coverage with subsidy, etc) It wanted to test with their plan data on the FFM system but that testing has been limited to 6 scenarios and has not yet begun; there are no plans to test the FFM SHOP marketplaces before Oct 1; they expect subsidy eligibility and back-end application processing to be fully on paper even if an applicant fills out the online application. They said this could potentially result in 30 -90 day delays between when an applicant fills out an application and when a plan is actually able to enroll the applicant in coverage with a subsidy reduced premium."

From: Tavenner, Marilyn (CMS/OA) [mailto:]
Sent: Monday, July 22, 2013 6:59 PM
To: Park, Todd; Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Re: BCBSA meeting; chatting tonight

Todd please call me if you want to talk. [REDACTED]

From: Park, Todd [mailto:]
Sent: Monday, July 22, 2013 06:57 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: RE: BCBSA meeting; chatting tonight

Apologies for the quick follow-on email would very much love to chat tonight for a few minutes; will make myself available any time; just name the time; thanks so much!

Todd

From: Park, Todd
Sent: Monday, July 22, 2013 6:51 PM
To: [marilyn.tavenner](mailto:marilyn.tavenner@cms.gov); Khalid, Aryana C. (CMS/OA); [michelle.snyder](mailto:michelle.snyder@cms.gov); [henry.chao](mailto:henry.chao@cms.gov)
Subject: FW: BCBSA meeting

Hi Marilyn, Aryana, Michelle, and Henry, hope you had a terrific weekend! I think you've already seen the email below, and you may already be writing up your thoughts on it... in whatever way is most time-efficient for you (including jumping on the phone for a few minutes tonight, if that is easiest), was hoping to get your thoughts to be prepped for the ACA outreach meeting tomorrow morning at 11 (if this comes up as a topic of discussion) [REDACTED]

What might work best for you? Thanks so much,
Todd

From: Siegler, Matthew [mailto:[REDACTED]]
Sent: Monday, July 22, 2013 05:03 PM
To: Lambrew, Jeanne; Hash, Michael (HHS/OHR) <[REDACTED]>; Nelson, Karen <[REDACTED]>; Primus, Wendell <[REDACTED]>; David Schwartz <[REDACTED]>; David Schwartz <[REDACTED]>; Aronson, Lauren (CMS/OL) <[REDACTED]>; Egorin, Melanie <[REDACTED]>; Miller, Erin <[REDACTED]>
Subject: BCBSA meeting

Hi All,

Sorry for the memory lapse, but the paper BCBS left with us did not go into specifics on the testing/readiness issues. They said they would send us that information. I've just pinged them about it and will share as soon as we have.

The specifics I wrote down from the meeting are as follows. BCBS claimed: there was a 90% failure rate on the initial "handshake" tests with issuers and the FFM; as of Friday BCBS had not been able to establish "full connectivity" with the FFM; HHS had scheduled testing of enrollment file transfers to begin on July 15 but that was delayed one week and is set to begin today; BCBS presented HHS with 23 eligibility scenarios (eg: family coverage no subsidy, single coverage with subsidy, etc) it wanted to test with their plan data on the FFM system but that testing has been limited to 6 scenarios and has not yet begun; there are no plans to test the FFM SHOP marketplaces before Oct 1; they expect subsidy eligibility and back-end application processing to be fully on paper even if an applicant fills out the online application. They said this could potentially result in 30-90 day delays between when an applicant fills out an application and when a plan is actually able to enroll the applicant in coverage with a subsidy reduced premium.

Thanks,

Matt

Matthew Siegler
Counsel
Committee on Energy and Commerce
Subcommittee on Health
Democratic Staff
[REDACTED]

Per our discussion and forwarded email from M. Siegler, here are key facts about the current state of engaging the issuers testing the enrollment functions of the FFM and Data Services Hub. My team and I believe that the first few bullets should illustrate the chronology of testing events/tasks since the end of May when the Trade Associations welcomed our revised accelerated testing approach. The last few bullet points attempts to objectively address the key issues raised by the BCBSA.

- **Acceleration of Issuer Testing Engagement Since End of May:** At the end of May, CMS announced to the issuer community a greatly accelerated FFM & Data Service Hub testing schedule, in which the key activities of issuer onboarding, connectivity testing with the Data Services Hub, issuer-initiated Direct Enrollment and FFM-initiated Enrollment transaction testing (834), and Plan Preview testing would launch with a series of thrice-weekly technical webinars in June and July, rather than waiting for those activities to occur in mid-to-late August as had been previously communicated. The Trades expressed their gratitude at the acceleration; AHIP called Aryana Khalid on May 21st after Henry announced the acceleration on May 17th to thank CMS and to say they knew what a heavy lift it was to move testing up.
- **Thrice-Weekly Issuer Technical Webinars:** Since May 30th, CMS has held 20 webinars and interactive Q&A sessions to engage issuers in the onboarding and issuer enrollment integration testing process, including the creation of the "CMS-Issuer Testing Technical Work Group" and "CMS-Issuer EDI Technical Work Group" webinars regularly attended by 200-300 participants per session, and each including Q&A between issuers and CMS's technical subject matter experts.
- **CMSzONE and CMS Technical Document Dissemination to Issuers:** Since May 30th, CMS has posted 58 technical guidance documents on CMSzONE, a secure, online repository for the issuer testing community, including the Issuer Onboarding Guide & Testing Handbook, Direct Enrollment Test Data documentation and EDI Test Files, onboarding instructions, issuer testing frequently asked questions (FAQ's) and all documents shared during the technical webinars.
- **Issuer Onboarding & Testing Steps:** In order for an issuer to conduct end-to-end testing they must accomplish three key activities:
 1. Complete an onboarding form that identifies how their respective system will connect with the Data Services Hub
 2. Complete configuration of electric file transfer (EFT) in the pushing or pulling of enrollment transaction files (EDI 834 transactions for example)
 3. Complete Web connectivity testing for those issuers participating in Direct Enrollment.

Of those three key activities, the following bullet points indicate where we currently stand and hopefully clarifies some of the issues that in some cases are non-issues:

- **Issuer Onboarding Status:** 143 issuers have submitted onboarding forms to date; however, of the issuers who have submitted QHP's directly in the HIOS system for the 19 FFM States, as of the end of last week, CMS is still waiting to hear from more than 60 issuers organizations who have not yet submitted a form at all the first step in the onboarding process that CMS launched in mid-June.
- **Most Issuers were not ready as of 7/15:** Based on our close monitoring of progress by Issuers, CMS made an announcement during the week before leading up to 7/15 start of testing, because of low percentage of issuers that have been able to complete connectivity testing (less than 10 issuers out of 75 issuers having completed connectivity testing before 7/15), CMS decided to extend the Connectivity testing until 7/19 and provide additional/focused technical assistance during the week of 7/15. From that effort, we've more than doubled the number of Issuers that are now ready for Integrated testing with FFM.
- **Issuer EFT Connectivity Status:** Of the 143 issuers who have submitted onboarding forms, 63 issuers have completed EFT configuration for the outbound and inbound receipt of 834 files; CMS is waiting on some information from 35 issuers in order to complete this step (and an additional 9 issuers who were just added via the onboarding process). When initially establishing connectivity with the issuers in early July, technical configuration issues were discovered on both the CMS and the issuer sides. In order to optimize the remaining testing time, and to avoid the time involved in individual configuration and troubleshooting, on July 18th, CMS began switching many issuers from a "push" to a simpler "pull" model in order to complete connectivity.

- **Issuer Web Services (Direct Enrollment) Connectivity Status** : Of the 75 issuers participating in Direct Enrollment, CMS is still waiting on 38 issuers who have not yet responded in supplying the required information to start the Web Services test. Of the remaining 37 issuers, all have been set up by CMS, and of those, 24 issuers have passed the Web Services connectivity testing.
- **SHOP Testing**: CMS has focused issuer testing first and foremost on individual Direct Enrollment and Enrollment 834 Transaction (834 is the HIPAA Standard Transaction for Health Plan Enrollment) testing as it relates to the individual marketplace, as this covers the broadest and most complex functionality in advance of October 1st. CMS has placed SHOP testing (as well as other aspects such as Lead Generation Testing) as a secondary priority once the former is underway. CMS does anticipate testing SHOP with the issuers in advance of October, and plans to hold a SHOP testing-specific webinar in order to launch SHOP variation of testing in mid-August. The SHOP testing will in essence be a simpler version of individual marketplace testing, as it does not entail the complications associated with eligibility, verifications, APTC or CSR calculations.
- **Scenarios**: CMS is making more than 23 direct enrollment scenarios part of the Direct Enrollment integration testing, including all of the scenarios that BCBSC had proposed. For 834 scenarios, CMS limited the overall scope to ensure that all issuers would be able to accomplish the required functionality during testing. Once all issuers are able to complete issuer enrollment integration testing, CMS plans to expand the number scenarios.
- **Enrollment File Transfers Testing** : After initial plans to begin testing of enrollment file transfers on July 15th, CMS began sending out the first 834 enrollment files to issuers on Friday, July 19th and has continued testing with the "Wave 1" issuers during the week of July 22nd.
- **Testing Dependency on State DOI Transfer of QHP's in Partnership States**: There are dependencies upon State DOI's to proceed in testing for those issuers in Partnership (SPM's) states and State Based Marketplaces (SBM's), because issuers can only test against those QHP's once they are transferred by the State DOI from NAIC's SERFF system to CMS's FFM system. The State DOI's have until July 31st to transfer the QHP's; until the QHP's for any given Partnership or NAIC State are transferred, only issuers with QHP's in one of the 19 FFM HIOS States will be able to participate in enrollment/834 testing with their QHP data.
- **Application Online Processing**: BCBSA mentions there are back end delays that could be 30 -90 days but they must have something mistaken or the thought was incorrectly captured because applicants that fill out the online application are not required to have the paper application filled out; their enrollments can be processed in a very short timeframe (e.g. 20 -40 minutes.)

From: Lambrew, Jeanne
Sent: Tuesday, July 23, 2013 9:38 AM
To: Tavenner, Marilyn (CMS/OA); Park, Todd
Cc: Khalid, Aryana C. (CMS/OA); Hash, Michael (HHS/OHR)
Subject: RE: Issuers

What do we do about the 25 Hill staffers who heard this information yesterday / many more who may still continue to be hearing this from the Blues through briefings?

From: Tavenner, Marilyn (CMS/OA) [mailto:████████████████████]
Sent: Tuesday, July 23, 2013 9:34 AM
To: Lambrew, Jeanne; Park, Todd
Cc: Khalid, Aryana C. (CMS/OA); Hash, Michael (HHS/OHR)
Subject: Issuers

We have heard again from AHIP that the "issues" are with the Blues.....and I am going to have both the Blues and AHIP in tomorrow with Henry et al and see if I can figure it out and make clear how we move forward. I would appreciate being able to do that first.....and would ask for your support. Thanks Marilyn

From: Park, Todd
Sent: Tuesday, July 23, 2013 9:40 AM
To: Tavenner, Marilyn (CMS/OA); Lambrew, Jeanne; Khalid, Aryana C. (CMS/OA)
Cc: Cavanaugh, Alicia A. (CMS/OA); Miller, Ruth A. (CMS/OA)
Subject: RE: Touch base on issuers

Just finished talking with Henry and team. Have additional content clarification, and also a clear sense of what we need to tell BCBSA in terms of how we all need to work together constructively going forward -- Marilyn, I think this would be useful info for you going into your meetings tomorrow with BCBSA and AHIP. I have to give brief remarks at an event at 10 am (for which I need to prepare now), but can talk at 10:30 am, or anytime between 12 and 3. Thoughts?

-----Original Message-----

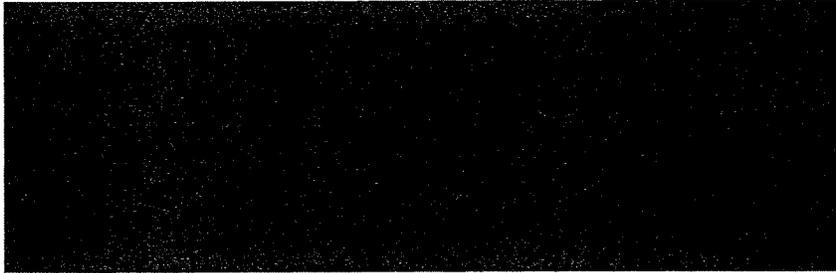
From: Tavenner, Marilyn (CMS/OA) [mailto:████████████████████]
Sent: Tuesday, July 23, 2013 8:48 AM
To: Park, Todd; Lambrew, Jeanne; Khalid, Aryana C. (CMS/OA)
Cc: Cavanaugh, Alicia A. (CMS/OA); Miller, Ruth A. (CMS/OA)
Subject: Touch base on issuers

Can we try for a conference call this am. Among us to discuss issues. Thanks.

From: Tavenner, Marilyn (CMS/OA) <[REDACTED]>
Sent: Tuesday, July 23, 2013 8:43 PM
To: Park, Todd; Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Re: Meeting today

Todd gave a great description of the meeting today [REDACTED] Having
Todd in our camp and knowledgeable is very very helpful!!

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, July 23, 2013 08:18 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Cc: Tavenner, Marilyn (CMS/OA)
Subject: Meeting today



On another front, close hold, as a result of the fire drill last night/this morning, and conversations that have been had with BCBSA/AHIP in its aftermath, it looks like substantial improvements will happen in terms of the dynamic on that front Marilyn will discuss with you in more detail. So hopefully that fire drill was not in vain.

Massive, massive, massive gratitude again for everything that Team CMS has done and continues to do may the Force continue to be with you, and God bless you,

Todd

LETTER SUBMITTED BY REPRESENTATIVE SCOTT PETERS



DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

NOV 14 2014

Administrator
Washington, DC 20201

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

As follow up to your September 18th hearing, I am writing to update you that the Centers for Medicare & Medicaid Services (CMS) resolved the 22 technical recommendations in the September 16th Government Accountability Office's (GAO) report, "HealthCare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls." We appreciate the GAO's work in this area and are using industry best practices to appropriately safeguard consumer's personal information. No person or group has maliciously accessed personally identifiable information from the site.

CMS will continue to strengthen the security of HealthCare.gov throughout its second open enrollment period. I hope you find this information helpful and I look forward to working with you in the future on this important issue.

Sincerely,

A handwritten signature in cursive script that reads "Marilyn Tavenner".

Marilyn Tavenner

cc: Ranking Member Elijah Cummings
Gene L. Dodaro, Comptroller General, Government Accountability Office

MINORITY STAFF REPORT SUBMITTED BY RANKING MEMBER EDDIE BERNICE JOHNSON

The View from “80,000 Feet”: Todd Park in the Run Up to Healthcare.gov



A staff report by the Minority Staff of the
Committee on Science, Space, and Technology
for Ranking Member Eddie Bernice Johnson
and the Members of the Committee's Democratic Caucus

November 18, 2014

The View from “80,000 Feet”: Todd Park in the Run Up to Healthcare.gov

To highlight the key findings of this report:

1. There is ample evidence that Mr. Park played a very limited role in Healthcare.gov. He was the person in the White House that others turned to when they had questions or needs related to progress on the program. This produced a voluminous record of queries from Park to the top management on the project at the Centers for Medicare and Medicaid Services (CMS). Park was engaged in the effort to reach out to diverse communities, to build excitement about gaining access to the healthcare Marketplace. CMS relied upon Park to assist them with interagency issues and in helping find resources when needed. None of that work could be described in any meaningful way as “substantial involvement with the development of the website’s privacy and security standards” or “intimately involved with the development of the Healthcare.gov website”. Those quotes come from the Majority’s staff report of October 28;
2. Having examined the complete documentary record from the White House, there is no record that shows Mr. Park receiving the normal management tools that would be an indication of intimate involvement in development. He did not receive the monthly progress reports from contractors, nor are there records of any involvement in setting contract requirements or giving managerial direction. There is no record that shows him engaged in technical efforts at understanding or shaping the design or coding of the Healthcare.gov web site. Those responsibilities were retained at CMS.
3. Based on a complete review of records, the Minority staff conclude there is no credible basis for an allegation that Mr. Park misrepresented his involvement in Healthcare.gov in his testimony before the House Oversight and Government Reform Committee on November 13, 2013;
4. Based on a complete review of records, the Minority staff conclude that there is no credible basis for an allegation that Dr. Holdren misled the House Science, Space, and Technology Committee in his representations about Mr. Park’s and OSTP’s involvement in cybersecurity in the development of Healthcare.gov;
5. The Science, Space, and Technology Committee’s Majority report of October 28, 2014, which made serious allegations suggesting that Mr. Park misled another Committee and Dr. Holdren misled our Committee, relied on a creative mixing of documents, from different people and periods of time, to try to create the impression that the allegations against Mr. Park and Dr. Holdren should be taken seriously. The Majority report also misquotes Mr. Park on a significant matter that unfairly suggests Mr. Park was not truthful in his testimony before another Committee—we recommend that Members seek to have the Majority correct that record immediately;
6. There is no evidence that Dr. Holdren had any meaningful involvement in Healthcare.gov issues, and Park does not include him in his circle of officials engaged in the education and outreach work on the launch of the Marketplace;

7. The Majority attempted to ambush Mr. Park in a fake “briefing” where they were going to surprise him with accusatory questions, selective documents, and a transcriptionist. When the White House, nervous about the transcriptionist, backed out, the Majority issued an accusatory report to push an unfair and unsustainable story-line that attacks Mr. Park’s veracity and his reputation. There is no justification for such disrespectful conduct towards Mr. Park.

BACKGROUND

This staff report is designed to provide background context and detailed documentary evidence regarding a hearing to be held by the Oversight Subcommittee titled, “The Role of the White House Chief Technology Officer in the Healthcare.gov Website Debacle.” This Committee has held two prior hearings on Healthcare.gov and has sent several letters related to the site to the Administration, but the focus of all prior work has been cybersecurity on the site.¹ The title of the upcoming hearing suggests that the Science, Space, and Technology Committee has shifted its focus from an area of clear jurisdiction, cybersecurity, to a broader set of questions about program performance. The program was managed and launched by the Centers of Medicare and Medicaid Services (CMS), an office at the Department of Health and Human Services that is not typically considered to be in the Committee’s jurisdiction. No officials at the White House had anything to do with the day-to-day management of the army of contractors who were responsible for carrying out all aspects of the project.

The Majority have telegraphed their messaging for this hearing both in their choice of a hearing title and also in a staff report released October 28, 2014. That report was titled, “Did the White House Knowingly Put Americans’ Sensitive Information at Risk? Committee Seeks to Clarify Contradictions Surrounding Senior White House Official’s Role in Developing Healthcare.gov.” That report makes several serious sounding allegations on very thin or tortured readings of an incomplete documentary record. The Majority report presents a pastiche of quotes and memos cited from different time frames, mixed together in clever but misleading ways, with many of the quotes in the report not involving Mr. Park at all and with no effort to clarify which of those things he may have known and which he certainly did not know.

Yet this stew of statements are woven together in a way that attempts to set the stage for a claim that both Mr. Park, the former Chief Technology Officer and Special Assistant to the President, and Dr. Holdren, the Director of the Office of Science and Technology Policy (colloquially, the President’s science advisor), misled the Committee on Oversight and Government Reform and the Committee on Science, Space, and Technology. The report quotes, and, in one instance, misquotes, Mr. Park to prove the central allegations of the report: that Park was “intimately involved with the development of the Healthcare.gov website.” and he had “substantial

¹ U.S. House of Representatives. Committee on Science, Space, and Technology. *Is My Data on Healthcare.gov Secure?*, Hearing. 19 Nov 2013. 113th Congress. U.S. House of Representatives. Committee on Science, Space, and Technology. *Healthcare.gov: Consequences of Stolen Identity*, Hearing. 16 Jan 2014. 113th Congress.

involvement with the development of the website's privacy and security standards". If those claims were true, Mr. Park could be accused of misrepresenting his position in testimony before Chairman Issa on November 13, 2014. And if the second allegation were true it may also lead to a conclusion that Dr. Holdren made misleading representations to this Committee. These allegations, if supported by documentary evidence or witness testimony, could potentially place Mr. Park in legal jeopardy. Given the large personal stakes for Mr. Park, the irresponsible way the Majority manipulate the record to try to support their incredible claims is especially disturbing.

Two of Mr. Park's quotes from the November 13, 2013 House Oversight hearing are made much of in the Majority report.

When Park was asked if, knowing how October 1 turned out, he would have asked to see the site launch "delayed or pushed back," Park responded:

"I don't actually have a really detailed knowledge base of what actually happened pre-October 1. I don't know what levers were available. So I would hesitate to make any point now."²

When asked about how much more testing of the website Park would have done prior to launching, the Majority report reads:

"I am not even familiar with the development and testing regimen that happened prior to October 1. So I can't really opine about that."³

This second quote is particularly threatening to Park because there is a significant e-mail chain of July, 2013 that shows Park getting a detailed account of development and (non-cyber) testing from Henry Chao (Deputy CIO, CMS) and Michelle Snyder (COO, CMS).⁴ This chain calls into question the seemingly absolute claim made by Park. However, **the Majority staff report, drawing from the "official" transcript produced by the Majority of that Committee,**

² "Did the White House Knowingly Put Americans' Sensitive Information at Risk? Committee Seeks to Clarify Contradictions Surrounding Senior White House Official's Role in Developing Healthcare.gov," A Report by the Majority Staff of the Science, Space, and Technology Committee, U.S. House of Representatives to Chairman Lamar Smith, Committee on Science, Space, and Technology and Chairman Paul Broun, Subcommittee on Oversight, October [28] 2014, p. 6.

³ Ibid, p. 6.

⁴ Exhibit 1 contains White House records that show a common pattern for Park: he is tasked by the White House to learn something; he turns to Chao and Snyder for information; then reduces their information into a bite-sized chunk. In this example he takes four pages of detailed testing and roll-out information from CMS and turns it into a 4 point Powerpoint slide for a White House briefing.

misquotes Mr. Park's reply. Instead of claiming he was "not even familiar", what Mr. Park said was:

"I am not deeply familiar with the development and testing regimen that happened prior to October 1."⁵

The official Oversight and Government Committee transcript is contradicted by commercial news service transcripts on this point. More importantly the recording of the hearing bears out that the Majority got it wrong, Mr. Park says "not deeply familiar". We cannot account for the transcription practices of another Committee, but our initial inquiries to the White House and suggest that the Oversight and Government Reform Committee did not submit the transcript to **them** for review. There is a world of difference between what appears to be an absolute denial of knowledge ("not even familiar") and a qualified denial of knowledge. The documentary record from the White House shows no reason to believe that Park's actual statement is at all inaccurate. The bottom line is that the Majority staff of this Committee used an inaccurate quote to try to make it appear Mr. Park perjured himself.

The Majority staff report made these poorly documented allegations before receiving White House materials from the critical months prior to launch of Healthcare.gov (May through October 1 of 2013). Now, the White House has turned over thousands of pages of documents that shed more light on Mr. Park's involvement in Healthcare.gov. Upon a review of that fuller documentary record, it is impossible to sustain an assessment that Park was, as the Majority report put it, "intimately involved with the development of the Healthcare.gov website."

"The bottom line is that the Majority staff of this Committee used an inaccurate quote to try to make it appear Mr. Park perjured himself."

Based on the most recent White House document production, it is easy to demonstrate that Park gathers a lot of information on a wide array of issues related to the program. However, using the description that he was "intimately involved" in the project implies a direct, daily managerial contact with the army of contractors. There is no document that shows such contact. In fact, the

⁵ Page 98 of the transcript from the Issa hearing with Todd Park has this quote – in response to a question from Congressman Gowdy about testing before the launch of the site on October 1st: Mr. PARK. I am not **even** familiar with the development and testing regimen that happened prior to October 1. So I can't really opine about that." In Part 2 of the video linked below, at about 22:15 seconds, in response to Congressman Gowdy's question on testing Park actually says: Mr. PARK. "I am not **deeply** familiar with the development and testing regimen that happened prior to October 1. So I can't really opine about that." <http://oversight.house.gov/hearing/obamacare-implementation-rollout-healthcare-gov/> Page 47 of the Federal News Service transcript, has Todd Park saying: MR. PARK: So I'm not **deeply** familiar with the development testing (regimen ?) that happened prior to October 1, so I can't really opine about that -- (inaudible).

documents reveal largely superficial contacts with contractors, usually mediated by CMS staff and focused on morale building rather than web design. This report highlights several examples of Park's real role--what it was and what it was not--and we are attaching over a hundred pages of previously unreleased White House materials so that people can come to their own opinion.

There is circumstantial evidence that the Majority has an animus towards Mr. Park, and that evidence rests on activities that are largely outside the public's view. In both the meeting of the Subcommittee to issue a subpoena for Mr. Park and in their staff report, the Majority make much of the fact that Mr. Park cancelled an appearance for a Subcommittee Member's briefing for scheduled for September 10, but they have not been transparent about what led to that cancellation or their plans for that event.⁶ In August, the Majority received documents from the Committee on Oversight and Government Reform that covered communications between HHS and Mr. Park. This Committee had not previously received those materials, and the Majority staff relied upon these materials to write their accusatory October 28 report. However, the Majority did not tell Mr. Park or the White House that they had received those materials. The Majority were even reluctant to tell the White House that they had engaged a court reporter to make a transcript of the "briefing." The Majority appeared to be welcoming Mr. Park to come brief them, while planning to get him into the room, without counsel and without notice that they possessed materials they believed would show he had misrepresented himself, and transcribe the confrontation. The Majority's planned September 10 ambush of Mr. Park was designed to place him in serious legal jeopardy. If this conduct does not telegraph animus, and disrespect, it is hard to know what would.

In evaluating the claims that Mr. Park was "intimately involved with the development of the Healthcare.gov website" and had "substantial involvement with the development of the website's privacy and security standards", one cannot lose sight of the fact that the development of the site was a product of contractual relations between CMS and the contractors on the project. By law, only CMS officials could set or change requirements and define deliverables. In none of the material provided to the Committee is there any evidence that anyone at the White House, and certainly not the Chief Technology Officer (CTO), took any step that directed requirements or deliverables. Nor are any of the usual documents used to maintain insight and control over a project--especially the monthly performance reports from contractors--found in the White House records.

In an interview with the House Oversight and Government Reform Committee, Michelle Snyder, the Chief Operating Officer at CMS (and Henry Chao's direct supervisor on the development project) was asked about Park's role in the development and she said this:

⁶ Withdrawal from the briefing is mentioned on the second page of the body of the Majority's staff report. "Risk?," p. 4.

“I would say with Todd, you know, Todd operates at a -- and again a good way to think of this is, if I say Henry is ground level, and I’m 40,000 or 50,000 feet, Todd is 80,000 feet.”⁷

The actual documentary record confirms Snyder’s characterization. The records demonstrate that Park did not have intimate day-to-day exposure to the program, the contractors, the development’s progress or problems, and he had no authority to tell anyone to do anything. He dipped in and out of Healthcare.gov as his leadership’s needs bubbled up or requests for help with resources or interagency issues came to him from CMS. He ended up covering a lot of different issues with the experts at CMS, but his involvement was not sustained and it was not a managerial involvement. He served more like a press secretary or legislative assistant--to use an analogy that makes sense in the context of Congressional offices--where he asked questions of the experts, gathered some materials from them and then boiled it all down to a powerpoint slide or a few bullet points for use with the press. Park’s exposure to the development of Healthcare.gov was wide but not deep, episodic not constant, and acting as a supporter not manager. Based on the documentary record from the critical months of May to October of 2013, the most accurate description of Todd Park on Healthcare.gov development is that he was a knowledgeable outsider to the development and validation of the website prior to October 1, 2013.

“(I) f I say Henry is ground level, and I’m 40,000 or 50,000 feet, Todd is 80,000 feet.”

Michelle Snyder, Chief Operating Officer, CMS

“Park’s exposure to the development of Healthcare.gov was wide but not deep, episodic not constant, and acting as a supporter not manager.”

TODD PARK AS CHIEF TECHNOLOGY OFFICER OF THE UNITED STATES

Todd Park left a highly successful career in the IT innovation world to join the Obama Administration, first (in 2009) as CTO for HHS and then, in March of 2012, President Obama named him Chief Technology Office of the United States. Park had co-founded athenahealth in 1997 and then in 2008 co-founded Castlight Health. Both firms were very successful working in the market space of providing information technology tools to make healthcare delivery more

⁷ . Transcript of Interview with Michelle Snyder by the staff of the Oversight and Government Reform Committee, December 3, 2013, p. 192.

effective and efficient. His co-founder at athenahealth was Jonathan S. Bush, a cousin of President George W. Bush.

The receipt of over 8000 pages of White House documents related to Healthcare.gov responsive to the Committee's request, is useful for the work of the Committee, but distorts Mr. Park's actual work. While no one denies that Mr. Park had contact with CMS regarding issues related to Healthcare.gov, it would be a mistake to pigeon-hole Park solely as the "HealthCare.Gov" guy in the White House. As CTO in the White House, Park oversaw multiple efforts to use IT and the internet as a means to make the government more responsive and transparent to the people, and to take steps to spur the spread and infusion of technology across the economy and society.⁸ While his position certainly gave him extraordinary insight into how things were unfolding in the development of an online healthcare marketplace, his attention was pulled across a wide range of initiatives simultaneously. The Majority are trying to define Park's job as solely about developing the online Marketplace, Healthcare.gov, but he did not have the luxury to work on that and nothing else for the months leading up to its launch.

Park led initiatives aimed at a wide swath of opportunities to use technology in creative ways. He was responsible for the Open Data initiative to put government data on energy, health, education, finance, public safety and global development online. He oversaw "My Data" which is designed to give citizens secure access to personal information about themselves with initiatives such as "green button"--where private sector energy companies make data about energy usage available to consumers. Initiatives to improve disaster response and to fight human trafficking also fell to the CTO. The CTO was engaged in "ConnectEd", an initiative to expand broadband access for k-12 schools and to improve training and course materials available to teachers for digital learning. The CTO was also supporting a wide-ranging effort to use the free up more spectrum to spur innovation and bring more, higher quality services to consumers and businesses. The CTO worked on internet policy for the Administration, including how to balance online privacy against the need for an open, innovative internet. Park established the Presidential Innovation Fellows program to attract bright innovators from the private sector to come work for up to a year with a paired innovative government official to address a targeted problem. The CTO also works on the President's "Open Government" initiative to make the government more transparent, responsive and collaborative.

These were initiatives "owned" by the CTO. In almost all of these areas, Park is overseeing an interagency process that would require a lot of collaboration, communication and cajoling of agencies to make progress. A fuller examination of Park's record of emails would reveal the breadth and energy of Park's involvement as CTO; Healthcare.gov was just a small piece in a very large pie. Park brought to his job the experiences of leading successful startups in the competitive, fast paced IT and venture capital world. His approach relies on "open innovation" or "crowdsourcing" and the "Lean Startup" philosophy of getting small, dedicated teams focused

⁸ Exhibit 2. This profile from the New York Times provides a good exposure to how Park was thinking about Information Technology challenges as CTO and the profile is not all about Healthcare.gov in large part because Park's job was much larger than just that.

on achieving what is doable, and then, through rapid innovation and continuous improvement, building out from that base. Park was trying to bring these values to his work across the board as CTO.

Park was pulled into work on Healthcare.gov by colleagues at the White House or at CMS when they had specific needs. He was clearly trusted by all sides to understand the challenges of a technology start-up, which is essentially what CMS was doing in their development of the website. However, he himself had a full time job just tending to the CTO's wide portfolio of initiatives and Healthcare.gov was very much a sideline that left Park at a very great distance from the day-to-day management of the project.

This is not to say that Park was not tempted to ask questions and brainstorm with technical people working on the Healthcare.gov project when he had the chance—he had been a brilliant developer in his start-ups. But he did not have the bandwidth to stick in that role, knew that too much interference would actually hinder the build being managed by CMS, and, on those rare occasions when he slipped up, CMS was not afraid to yank his chain and tell him to back off.

9 EXAMPLES THAT TODD PARK WAS NOT INTIMATELY INVOLVED IN DEVELOPING HEALTHCARE.GOV

The attached documents are designed to let fair-minded readers form their own opinions, but we believe that the evidence on Park's role is very clear and can be well illustrated with nine examples.

1. Park and the White House Could Not Direct Contractors

On June 29, 2013, the Deputy Chief Information Officer at CMS, Henry Chao wrote to Park regarding a meeting Park had with a subcontractor, Ideo. Chao wrote,

“I wanted to talk to you about a meeting you had with Ideo. Apparently something was misinterpreted from what you said and the top dog you met with circled back to OC [the CMS Office of Communications; OC was in charge of certain key elements of the user experience interface] and started to work on an alternate rendering of the paper form as if they were instructed to follow a different set of requirements. This is a pretty big issue since Ideo does not get to change requirements and scope without it coming from CMS directly. If there's anything you can do to help clear this up we would greatly appreciate it, or rather the program would appreciate it since it will hold the line of confusion and risk.”

Park responds, “Will work on making (this) happen as you've requested and report back!” Mary Wallace, Deputy Director in the Office of Communications at CMS reinforced Chao's message:

“... I think the real concern is to not have contractors trying to interpret what they think you or others from HHS or the White House asked them to do. The biggest

help would be for all of you to carry the message that the best thing IDEO (or any contractor) can do is what CMS is asking them to do... We have a lot of contractors supporting this effort and we are working hard to keep them all on the right track to get everything done in time.”

Park responds: “Hi Mary, thank you for the flag, will absolutely do!”

Todd reports back that same day, “Hi team, just pinged Team IDEO (including the CEO) and said that they should be sure to follow CMS’s lead, and that CMS is the unambiguous operational leader of all of the Marketplace work, in case that wasn’t clear ☺... But what I’ve clarified in our follow-up ping is that we are going to circle back with CMS on this (to understand current UX [user experience] decisionmaking process and if any further support/air cover for user-centric-ness is needed on an ongoing basis...)” There is no evidence that this “circle back” ever happens, and as the record revealed, Park himself could not get a hands-on user experience of the website until September. However, this exchange shows that CMS was **clearly** in charge—the keepers of requirements and scope on the project and the only ones with the power to direct contractors. It also reveals that Park’s natural orientation is not towards a deep understanding of the scope and requirements of the contract or an appreciation of the challenges of managing and integrating a large team of Federal contractors; those issues, which lie at the heart of what was delivered on October 1, were solely the domain of CMS.⁹

2. CMS Refuses Park’s Offer to Help with “Creative Solutions” on Spanish Translation

On September 12, Park sends a note to Marilyn Tavenner about why the roll-out of functional Spanish language translation for the Healthcare.gov site would not be ready by October 1. “Macon (Phillips, White House Director of New Media) pinged me, and asked what the root of the technical issue was and if a creative solution might be possible. I said that I would check with you ☺ Might you be able to circle back with your tech team on this question? If it would be even remotely helpful, I would be more than happy to join the technical conversation as well.” In a follow up e-mail that same day, Park writes, “To help with internal understanding here at the WH (and therefore with mobilizing energy and help for external messaging!) would you mind if I got on the phone with Henry [Chao] for 5 min to get a quick download on the tech details?”

Tavenner says, “Yes, but go through Michelle [Snyder--the Chief Operating Officer at CMS] first... Todd I need folks to understand the VERY best way they can help us -is to reach out to the advocates -educate them and garner their energy/support.” Tavenner loops in Aryana Khalid [Senior Advisor to Snyder] of CMS who responds to Park and closes with: “I know you are trying to help us and we so appreciate it. What we need is folks focusing on what they can do which is the messaging and talking to the advocates, not focusing on the IT or trying to come up with creative solutions to solve this. I hope this makes sense.”¹⁰

⁹ Exhibit 3.

¹⁰ Exhibit 4.

“What we need is folks focusing on what they can do which is the messaging and talking to the advocates, not focusing on the IT or trying to come up with creative solutions to solve this.”

Aryana Khalid, CMS to Todd Park, White House, CTO, September 12, 2013

Note that at this point, Park feels the need to ask permission to interrupt Henry Chao, who was doing the day-to-day management of the contractors on the project, to get 5 minutes to pursue this question. How can anyone seriously think Park is intimately involved in carrying the technical side of the program to completion? In any case, the response to his offer of technical assistance is a very clear message to stay in the lane of education and outreach and not to get in the way of delivery on the system through technical interventions. Park does not press his offer.

3. Chao Kills “Open Innovation” on Healthcare.gov

The start-up philosophy that was espoused by Park and others at the White House ran right into the wall of Henry Chao’s awareness that he had to build a site that would meet federal security standards and not multiply opportunities for fraud. In this clash of cultures, Chao was a clear winner.

On June 22, David Simas (WH Deputy Senior Advisor for Communications and Strategy) starts a long e-mail chain titled “this is great” about a blog post by Alex Howard. He sends his note to Park and Tara McGuinness (Senior WH Communications Advisor working Healthcare.gov). Park replies, adding Bryan Sivak (CTO/HHS) to the chain.

“I believe what Alex Howard is discussing in this (great) piece is the new Healthcare.gov content site, which is up and running, and for which the code has been posted on Github (an online repository for open source code). The content site will front-end the Marketplace -- but the actual Marketplace eligibility-checking/enrollment/plan compare functionality is not up yet. Bryan, can you confirm/elaborate? Thanks!”

Sivak offers a long reply that includes:

“we are going to publish the code this week... if you take a look at the /developers page you’ll see that we have detailed the programmatic mechanisms for accessing content, but have a “coming soon” where the links to the GitHub

repos are... This is a paradigm shift for the federal government and the fact that its happening on Healthcare.gov is a really big deal for the tech community.”

There is more back and forth on this, focused primarily about how to get the word out about this innovation to the technology press/community, but the basic point is that letting other developers look at the code can be used as a means to quickly optimize performance and even expand functionality. This is a clear manifestation of a private sector approach of “crowdsourcing” innovation applied to the government. Github’s slogan is: “Build software better, together.”

However, Henry Chao weighs in a few days later. On June 28 he writes to a long list, including Sivak, Park and all the key CMS people:

“I want to express my reservations about putting nearly all the source code for the hc.gov/Marketplace Portal Website on Github and making it available for absolutely anyone in the entire world to use. While in its current state it does not contain the code for the Online Application, someone with less than honorable intentions can easily stand up a shadow site that would fake out the general public and they can do it easily and literally in just a day or less. While I believe and support sharing and being open about our codebase I think we have to balance that with safeguarding security, privacy, and the public trust.”

That email squashed future GitHub releases of code and the sensitive “backend” of the program was never put up.¹¹ This chain illustrates the culture clash between the entrepreneurial practices from Silicon Valley and the complex statutory and regulatory environment that the day-to-day managers of a multi-billion dollar acquisition know they have to live with.¹² In this area, the second set of considerations trumped the “innovation” of the first set of values. Also, one can’t lose sight of the fact that the discussion around this matter is about how to work the press to get maximum exposure for progress on Healthcare.gov.

4. Park Not Welcome at July “Readiness Review”

In July, Park spends five hours in a “deep dive” briefing with Henry Chao to understand how development of the Marketplace was proceeding (this appears to be the only “deep dive” between July 1 and October 1). Chao would have been boiling down hundreds of hours of work across the full array of development issues to give Park a sense of where they are because Park did not have that kind of time to give to the project. Park asks if he can attend one of the upcoming Readiness Review meetings that was to be an end-to-end walk through to cover where things stood with CMS and all the contractors. Chao initially seems to agree because he has Todd’s scheduler engaged to set time aside for Park.

¹¹. Adrienne Jeffries, “Why the government unpublished the source code for Healthcare.gov,” [The Verge](#), October 18, 2013.

¹² Exhibit 5.

In an email that goes to Tavenner, Khalid, Snyder and Chao, Park writes:

“I am very much looking forward to being a fly on the wall at the E&E readiness review on the 19th. I’ll be able to attend from 11 am to 4 pm... David Simas is very interested in being a fly on the wall for a walkthrough of the FFM web workflow, and also would love to soak up a sense of the underlying complexity of the overall Mktplace machine.... he would really appreciate the opportunity, and/but also doesn’t want to disrupt things in any way.... (FYI, I’ve briefed him in detail about the fact that we’ve locked down business requirements and are in pure operational execution mode for Oct1/Jan 1). Thoughts?”

“Flys on the wall are seldom invisible and often distracting!!!”

Michelle Snyder to Todd Park about attending an all-contractor readiness review on July 19.

It takes 9 minutes for Snyder to respond:

“We need to talk abt (about) attendance at readiness reviews. I am sure you can anticipate my position on that. Flys on the wall are seldom invisible and often distracting!!!!”

Chao weighs in half-an-hour later:

“My recommendation is that the readiness review in which we conduct (sic) is not really conducive for being an observer at this point and we should stick to the briefing format for you at various intervals.”

Park then graciously withdraws from the event.

5. Park Can’t Get a Hands-on Walkthrough of Healthcare.gov

Beginning in July, Park asks Snyder and Chao if he can come do a walk-through of the live system. First he asks for a hands-on “tour” in Baltimore for August 5. After much negotiation (partly because others from the White House want to come), they set a time for the evening of August 8. On August 2, Chao writes to Park saying that Snyder has advised that the WH tour should be combined with a similar visit by Marilyn Tavenner expected to happen the week of August 26. Park says fine and explains to his colleagues that the exercise was being postponed. On August 22, Tavenner writes that she is on vacation that week and would look to do a walkthrough the week of September 3. **So the live experience of the system Park tried to arrange for early August did not occur until at least September 3.** It is hard to reconcile the claim that Park was deeply involved in the development of Healthcare.gov with the reality that

Park could not even get access to the web site experience as it was being developed. And when he finally gets what he asked for does it is in the context of a big group visit.¹³

“It is hard to reconcile the claim that Park was deeply involved in the development of Healthcare.gov with the reality that Park could not even get access to the web site experience as it was being developed.”

Keeping Park on a short leash for his contact with technical people, precisely to guarantee that he does not distract them from their tasks, leads to this amusing exchange regarding a September 24 visit to the Herndon center. Snyder writes to Chao, Park and Tavenner:

“I have requested that the security cameras at Herndon be loaded with facial recognition software so that if either of you [Park or Tavenner] wander into a restricted area armed with a set of questions alarms will sound...”

Park responds: “Will absolutely obey all instructions with precision!! And really looking forward to the visit -- and more than anything, thanking everyone from the bottom of our collective hearts for the truly incredible work they are doing ☺” Tavenner reports back later: “I kept Todd under control (well sort of). Henry thanks for a great visit!!!”¹⁴

6. CMS Uses Park to Help When They Have WH, Interagency or Resource Issues

Park intervenes on several occasions to help CMS (most often at the behest of Henry Chao) out of jams of one kind or another. Park is tireless and uncomplaining when given these tasks and clearly views it as something he can do to help create the space for CMS to succeed in managing the program. Park speaks directly with Blue Cross and Blue Shield executives about why logos cannot be integrated into the site by October 1, and also lets WH staff who may be interested in helping BCBSA push back know that it could create program risk.¹⁵ Park helps Henry in August by arranging a call with executives from RedHat to make sure their very best people are put on Healthcare.gov development, and to ask for very specific types of specialists that Chao needs.

¹³ Exhibit 7.

¹⁴ Exhibit 8.

¹⁵ Exhibit 9.

When it succeeds, Park offers to contact the Federal agencies who would be losing some of those specialists in the “surge” around Healthcare.gov and also says if they need any other “surges” to just ask and he would pitch in to help make it happen.¹⁶ A few days before the system goes live, Tavenner asks Park to contact the state-based markets leaders--clearly a task she was to do but felt she could not make time for. He spent two days tracking all 15 state IT leaders down and reported back.

In the last days before the Marketplace was to go live, Chao contacts Park to see if the White House can help arrange transport of server hardware from Florida to Culpeper, Virginia so that the communications center CMS had there could handle the expected volume of consumers logging onto the site. Park dutifully goes up his chain to see what is possible while helping them try to find a private sector solution. In the end, Verizon and CMS find that FedEx can do it using a special service and they go with that option.¹⁷ Park’s behavior clearly shows that he views himself as a resource multiplier for CMS, and he is always ready to throw his weight behind their requests for help.

7. Park is an Information Aggregator for the White House: Cybersecurity 1

As CMS uses Park to mobilize assistance from the White House -- provide “air cover” in Park’s phrasing -- staff at the White House turn to Todd Park to get information from CMS on a host of issues related to Healthcare.gov--records provided to the Committee show him doing this on development in July for a WH briefing and on Hispanic community outreach in September. However, much has been made by the Majority of Park’s “involvement” in cybersecurity, and so we believe that matter should be dealt with in detail. A review of the broad documentary record provided by the White House makes it very clear that Park is engaged in this matter in the August-September timeframe in response to concerns by the people he works for at the White House who desire to have a clear, convincing message on security. The White House was very aware that the press and Republican Members of Congress, were starting to spin up stories about the security of the site and so it was natural for White House staff to get up to speed on the development’s progress and to directly address any interagency needs for policy. At this time, there is also a report out from the HHS Inspector General about testing and security of the Data Hub part of the development for Healthcare.gov.

Park’s communications throughout this time clearly reflect his role is almost exclusively about message development and information gathering. He most definitely was not managing cybersecurity development of Healthcare.gov.

In August, the WH begins to ask questions regarding cybersecurity and privacy; Todd Park is tasked with gathering information. Park turns to the experts at CMS for help. On August 23, he writes to Michelle Snyder, Tony Trenkle, and Marilynn Tavenner with a subject, “Cybersecurity bullet points needed.” **“WH folks would love to get three basic bullet points describing how**

¹⁶ Exhibit 10.

¹⁷ Exhibit 11.

we will protect the Marketplace from cyberattack. Many apologies, but if we could get these by COB today, that would be fantastic is that possible? Below are three strawcase bullet points folks have drafted feel free to edit/change any way you see fit. See notes following each bullet as well.”

It is not clear that Park even drafted these bullets, but the questions he writes are revealing of his lack of confidence in the points. On the first point he notes, “want to make sure this is stated/framed accurately.” On the second point he writes, “you may want to replace this bullet entirely with another bullet that describes CMS’s cybersecurity approach and capabilities. If you want to add more than one bullet on that, that’s also totally cool.” In the event, CMS rewrites all three points with the first and second point reflecting substantially new information.¹⁸

This exchange sets the stage for an email thread titled, “Cyber next steps,” which is made much of in the October 28 Majority staff report’s effort to paint Park as intimately involved in decisionmaking around cybersecurity. The origins of the string are not clear in the materials included in the Majority’s report, but documents provided by the White House suggest there was a push to get a coherent message together due to external inquiries. The first email is from Park to Tony Trenkle with a cc to Michelle Snyder and it lays out three points. The first point is:

“We should convene a work session in the next week with you, Teresa, Frank Baitman [CIO at HHS], his CISO, and probably a DHS person and DOJ person (she [Snyder] was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don’t want to be a scheduling bottleneck, and it should really happen sooner rather than later... You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!”

“I would absolutely love to be part of as much of this meeting as I can, but also don’t want to be a scheduling bottleneck, and it should really happen sooner rather than later.”

Park to CMS staff in discussing the need to have an interagency meeting on cybersecurity and the Marketplace, August 28, 2013

Park’s note makes clear that he does not view himself as central to the substance of the cybersecurity discussion that is proposed—the conversation can go on without him. That is not the attitude of a person who is directly involved in shaping cybersecurity aspects of Healthcare.gov. And the point of the meeting would be a memo for the White House that lays out response steps for protecting the site from malicious attack.

¹⁸ Exhibit 12.

Later, that very same day (August 28), he again writes to Tony Trenkle, Michelle Snyder, Frank Baitman and Aryana Khalid:

“Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by the end of next week to help inform the memo will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.”

This email puts the first one in the chain in a clearer light. White House concerns about having a strong, clear message on cybersecurity, and making sure there was a coherent interagency strategy, drove Snyder, Trenkle and Park to begin planning. What must have been an interagency meeting provided Park with more clarity about exactly what was desired by the WH for the memo.

The idea that it was an interagency meeting on ACA is confirmed by an email on August 29 from Edward Siskel (White House Counsel) to a long list of White House staff (Todd Park is among them) and including representatives from Justice, HHS, the Federal Trade Commission and probably DHS. Siskel wrote, “Thanks again for participating in yesterday’s meeting and for all the work you have been doing to help protect consumers during the roll-out of the Marketplaces. Below is a list of do-outs from the meeting based on my notes.” All of the to-do’s on this document have to do with public education materials regarding fraud and an effort to identify external validators who can speak to “public education/outreach, intake process, value of Sentinel, prosecution, etc.”

There are several places in the records where Park helps locate or asks for “external validators.” This is a strategy whereby a quotable expert is found who can confirm for reporters that a

particular plan or point is credible. This is a common technique that is used in Congress as well as the White House. When a story is pushed out, those doing the pushing also provide the names of experts who can speak to the credibility of the claim to “validate” the story.

Starting September 2, there is a (relevant) new thread started by Todd Park in an email to Chris Jennings, the President’s Senior Healthcare advisor. The email contains “cybersecurity background points for (redacted).” We know the redacted meeting referred to was a scheduled Presidential briefing. Park shares the same points developed by CMS on August 23 with a few updates from the August 28 initiative. Jennings writes back to Park:

“Ok, thanks Todd. Quite helpful and will serve as a placeholder for (redacted) We need to have all of this locked down for the September 11th hearing we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards sand how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.”

Park shares with CMS people looking for more details on the idea that federal standards are more rigorous than private sector standards. At 1:38 am on September 3, Park sends to Jennings an expanded set of bullet points that addressed Jennings’ question. These were done up by Frank Baitman (HHS) and Tony Trenkle (CMS). Later, Chris Jennings writes back to everyone to thank them for their help and to report the meeting went well.¹⁹

Instead of being a decisionmaker on cybersecurity, Park is involved here in what is an effort to prepare external messages and firm up interagency coordination on policy because of increased attention on The Hill and in the press. Significantly, nothing in these records suggests that Park is drilling down into the development of cybersecurity tools in the Healthcare.gov website, or the testing of those methods or anything of substance about FISMA requirements--the things that the Committee has had testimony about in prior hearings. When Jennings refers in his September 2 email to how Federal websites have more rigorous security standards than the private sector, Park cannot respond in substance, but has to send it to CMS to handle the issue. Time and again, he turns to CMS for expert knowledge in an area he is not expert in to

“Significantly, nothing in these records suggests that Park is drilling down into the development of cybersecurity tools for the Healthcare.gov website, or the testing of those methods, or knows anything of substance about FISMA requirements”

¹⁹ Exhibit 13.

inform the work of the White House. It is absurd to try to turn any part of this exchange into some evidence that Park had a substantial role in managing or developing cybersecurity code, requirements, standards, testing or performance for the website itself. An important point to note: Henry Chao, who is so often Park's contact on CMS issues, is not in charge of cybersecurity development for the site.

8. Park as a Spokesman: Cybersecurity 2

Not to diminish the value of spokesmen, but in complex, modern organizations they are rarely the principals in carrying out policy or directing resources. In his CTO hat, Todd Park often played the role of spokesman to the press regarding IT initiatives for the Administration. There are multiple examples of Park seeking information from CMS (not directing them to do things, but asking for their help) about Healthcare.gov in preparation for media contacts, but because cybersecurity is so important to the Majority's (mis)characterization of Park, it is important to examine an example of how Park worked with CMS to prepare for a press call.

On September 17, the Healthcare.gov team at the White House finished up editing and clearance on a press release entitled, "Obama Administration announces a coordinated interagency effort to prevent and detect consumer fraud in the Health Insurance Marketplace." This is obviously a release which has its roots in the education and outreach effort Park participated in as discussed above in item 7. The Office of Communications sets up a background call with the press for September 18. Park writes to Jessica Santillo of White House Office of Communications,

"Hi Jessica, I'm signed up to help with the call! Looping in Tony [Trenkle], Frank [Baitman], and Brian [Cook of CMS]. Two questions: 1. Is the call on background, or on the record? 2. Can Tony Trenkle and Frank Baitman join me on the call? They are the folks who know the details, and it would be super-helpful for them to be on."

Initially Santillo says that is fine and tells him the call will be on background according to "White House officials". Then Communications decides the call should be WH only leading Park to write to Trenkle, Santillo, and Baitman (as well as others at CMS)

"it looks like the background call tomorrow is with WH folks only, with detailed inquiries to be referred to agencies... I've let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can talk to it at a general level only."

"I've let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can talk to it at a general level only."

Park to Santillo, Trenkle, Baitman regarding an upcoming press call, September 17, 2013

This tone of acknowledging that the website technical experts reside at CMS is completely consistent with everything Park testified to before Chairman Issa on development more broadly and also is consistent with subsequent characterizations made by Dr. Holdren to this Committee.

Park sends around talking points on cybersecurity for their review, but acknowledges they are drawn from the past materials that had already been worked up on the issue—meaning that CMS had already approved (and re-written) much of it before. The next day, September 18, the day of the call, Park writes to Trenkle and Baitman with additional questions. These are significant because they demonstrate the state of Park’s confidence in cybersecurity matters just two weeks before the roll-out of Healthcare.gov. The first question:

“And Tony, one more background question: is it the case that the security testing is done by an independent contractor managed by CMS info security staff, and that the review of results, assessment, and signoff happen via you, the CISO, and CMS info security staff? Thanks!”

Twenty minutes later he sends another email,

“And Tony and Frank, sorry, one more background question: the press release today says: “Together with our interagency partners, CMS has developed a rapid response mechanism to respond to a potential data breach and mitigate the effects of attempts to jeopardize the integrity of the Hub and the database it connects” Is this the same thing as the Incident Response capability discussed in Marilyn’s letter, but with souped up interagency coordination? Or is it something different?”

Trenkle confirms that he has both characterizations right. Baitman also sends a reply, but it is responding to another question that Park had buried in his draft talking points about how many Authority to Operate (ATO) security certificates would be issued for Healthcare.gov. Park thought there would be multiple ATO’s issued; Baitman says just one for whole system—this key point Park got wrong.²⁰

It is significant that Park is uncertain about these very basic points. Anyone substantially involved in the cybersecurity side of Marketplace development would know these matters inside and out—they are sort of cybersecurity 101 questions. The fact that Park does not seem to know who the security testing contractor is—typically in this kind of note he would mention the company—is another “tell” that Park is working in the shallow end of his knowledge pool. These questions illustrate that an effort to describe Park as intimately involved in cybersecurity development is simply ridiculous. **Not to lose sight of the obvious: Park’s only reason for another crash course on cybersecurity was to serve as a spokesman with the press as a “White House Official” explaining the Administration’s initiative.**

²⁰ Exhibit 14.

9. Park Brings the Cupcakes: Tending Team Morale

On the 28th Park writes to Chao: “I have permission from Michelle (Snyder) to bring y’all food tomorrow (the 29th) in Herndon on the condition that I leave immediately after delivering the food and not involve you in a long and super-interesting conversation that takes time away from your incredibly important work ☺” Park offers to bring lunch or dinner, but Chao indicates meals are covered and tells Park, “you are in charge of the out of the ordinary surprises.”

Park goes to Georgetown cupcakes to get 150 cupcakes and Haagen Daz for ice cream. He tells Chao that his father is driving him to Herndon, and that he will deliver the food and leave. Chao responds: “I think you can come in and help dole out the food and say hello. People here want to be able to at least see you in person. It really makes them feel like someone cares enough about their contribution to do this kind of thing so come in for at least 30 minutes but don’t wander to where the architects and engineers... are because they will never let you leave.”²¹

“People here want to be able to at least see you in person. It really makes them feel like someone cares enough about their contribution to do this kind of thing...”

Chao to Park bringing 150 Georgetown cupcakes to lift morale at the Herndon site on September 29, 2013

This small anecdote sheds light on the way that Chao used Park on several occasions: to inspire the various teams working to get Healthcare.gov up and running. Park was an ambassador from the White House and he invariably tried to bring food. The email record is full of offers of Park to bring humus, cookies, cupcakes at the drop of a hat. And from all written accounts, Park is passionately enthusiastic and grateful for the hard work the teams were doing.

Anyone who has led groups of people through hard tasks -- any kind of campaign, for example -- knows how important small acts of kindness and appreciation are to keeping people motivated and moving forward. Park played this role very, very well.

Even at the very end, Park was trying to inspire people to great efforts to make October 1 a success. At 11:02 pm on September 30, Park sends an email to a string of top CMS and Verizon/Terremark, CGI recipients. Because it is so revealing of Park’s attitude and personality, it is worth quoting from at length.

“Dear Laura, David, and Chris, thank you so very much for the heroic work you have done and are doing to support Marketplace go-live! We have one more favor to ask:

²¹ Exhibit 15.

I understand from Henry that a Verizon/Terremark team is working very hard to activate all the new hardware that's arrived at Culpeper. Every new VM, every ounce of additional power adds materially to the probability of a successful go-live tomorrow morning. If there is any possible way that you could 2x, 3x, 4x progress by having teams work in parallel tonight, that would be absolutely amazing. Possible? This is a historic moment, and the team is so very close to pulling off a feat for the ages is there any way to amp things up even further? We would be massively, massively appreciative please contact Henry with questions/thoughts!"²²

Here Park is playing his role as an inspirational voice asking for the last, best effort from those on the front line, without undermining CMS's authority. In the end, there was only so much exhortation could do to bring the new servers on-line, and it is highly unlikely that insufficient hardware was the sole issue that contributed to the problems on October 1. The problems on October 1 are precisely what led Park to be pushed out of his roles as aggregator, advisor, supporter and spokesman -- roles appropriate to the months leading up to launch -- to join a small team working to get down into the guts of the web site to analyze what was wrong and how to make it right. In that, they succeeded, but that success is not of much interest to the Committee.

CONCLUSION

Looking at the record: Park was not to give contractors direction, was not welcome at the readiness reviews, was not able to get a hands-on walkthrough of the web experience, was turned away on offers to help with technical problems. Time and again he is pushed by senior CMS officials back out of technical discussions or too much on-site time and back to his 80,000 foot orbit. He appears to take these nudges with grace.

The thousands of pages of records simply do not sustain a claim that Mr. Park had "substantial involvement with the development of the website's privacy and security standards" or was "intimately involved with the development of the Healthcare.gov website" as the Majority Staff Report framed their allegations. To believe these allegations you have to ignore all the examples offered in this report of what Park was not allowed to do by CMS. To believe these allegations you have to distort the record into unrecognizable form. To believe these things requires that a person know absolutely nothing about how multi-billion dollar Federal software acquisitions are managed. None of the normal signs of substantial or intimate involvement in that management—communications around requirements, critical path progress and key technical issues, changes to scope, work orders, spend rates—can be found in the records involving Park. The anecdote about his conversation with Ideo, and the pushback he got from Chao, is as close

²² Exhibit 16.

as the record comes to showing Park interacting on program details with a contractor, and in that case Park is schooled on staying in his lane.

In an interview with the staff of the Committee on Oversight and Government Reform, Henry Chao was asked about Park's involvement in development of the website:

"Counsel: ... he [Park] wasn't involved in the day-to-day management of the Federal marketplace. Is that correct? The IT?"

Chao: Correct. Not managing it. I think he was, of course, you know, part of the overall what I would consider the senior leadership, the technical leadership anyway, for the Federal Government, of which there's a natural alignment that needs to occur between all technical kind of issues, because of his role.

But he didn't own anything, meaning, you know, he didn't have the budgets, the staff, the contractors. So the day-to-day management really still falls to the operating agencies that are kind of trying to implement the program. He served as --advises on issues, helps you air certain cross-cutting issues, create, I believe I mentioned this, a forum to discuss and collaborate on cross-cutting issues... Interagency. Or even interdepartmental in some cases. So, you know, he's best suited, you know, to kind of do that role because of his position.

....

Counsel: So he would check in and have conversations to see what was going on, but he wasn't necessarily, how do you put it, like on the ground looking at -- looking at code, looking at --

Chao: No. He -- yeah. He doesn't provide direction... He's not, you know, officially in the chain of command, you know, because I take my direction from Marilyn Tavenner and the center director of CCHIO, and the chief information officer and the chief operating officer of the agency."²³

Todd Park did do a lot of work related to Healthcare.gov. The record makes abundantly clear what Park's role in Healthcare.gov was prior to October 1, 2013. He was the chief support for CMS needs within the White House, and was the chief representative for the White House when Chao was looking for a cheerleader to come inspire the teams. He was an asset with the private sector both in outreach on ACA, but also when Chao was looking for access to top contractors who could help his program or when there was a need for external validators. The vast majority of email communications between Park and CMS, most frequently Henry Chao and Michelle Snyder, are requests for information driven by Park's own need to provide information to his leadership within the White House or to be prepared to interact with the press or public as a spokesman for the White House. In all of these roles, Park excelled. On balance, the records

²³ Transcript of Interview of Henry Chao by staff of the Committee on Oversight and Government Reform, July 22, 2014, starting on p. 78.

show Park to have been endlessly energetic, enthusiastic, creative, and optimistic. But on technical questions related to the development of the website prior to October 1, we are convinced that “knowledgeable outsider” is an accurate description.

Mr. Park has already enjoyed a successful career as an IT entrepreneur and job creator. He gave that up for a few years to come to Washington to improve the performance of the government in delivering services to the American people and to try to improve our country by pushing innovation to address social needs and economic opportunities. Based on the thousands of pages of records and his prior testimony, he did nothing wrong at any stage of his relatively short public career. We can find no basis for alleging that he misrepresented himself before the House Committee on Oversight and Government Reform, and absolutely no evidence that he had a substantial role in cybersecurity development. That should also dispose of the allegation offered in the Majority’s staff report that Dr. Holdren misled the Committee in his communications about Mr. Park’s involvement in developing cybersecurity standards and tools for Healthcare.gov. As to Dr. Holdren himself, there is absolutely no indication in the White House records that he had any role in Healthcare.gov. So far as we could determine, Dr. Holdren is on none of the email chains involving Park and CMS. The bottom line is that the records in our possession appear to exonerate both Mr. Park and Dr. Holdren of the allegations made against them in the Majority staff report.

Exhibit 1

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Saturday, July 13, 2013 8:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA)
Subject: Testing information
Attachments: testing summary to Henry 07 12 2013.docx
Importance: High

Attached is the requested information you asked for on testing.

Let me know if you need anything else.

Thanks

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

CMS is testing with each business partner of the Federally Facilitated Marketplace (FFM): (1) Issuers; (2) States; and (3) Federal Agencies. The tests are designed to ensure that each partner can connect to the FFM IT systems and exchange data properly to support the actions a consumer takes to enroll in a Qualified Health Plan (QHP) on the FFM or to be transferred to a State for Medicaid/CHIP Enrollment:

- Issuer testing validates that issuers and the FFM can orchestrate the enrollment of consumers into plans on the FFM;
- State testing validates that States and the FFM can transfer consumers between the FFM and States depending on eligibility for the Health Insurance Marketplace or Medicaid/CHIP.
- Federal Agency testing validates that the FFM, through the Data Services Hub (DSH) can exchange the data required for eligibility determinations.

General Testing Approach

- CMS has developed a test plan, schedule, and data for each set of external partners. The test data is designed to test the critical business rules for eligibility determination.
- To prepare for Federal Agency Testing, CMS developed and utilized a Test Harness to simulate responses from the Federal Agencies. This approach allowed CMS to detect and correct software issues in the FFM prior to testing with other Agencies.
- All external partners will begin End to End testing in Mid-August with planned end date of August 31

STATE

- States have been involved in "Wave" Testing since March of 2013. The Wave concept onboards States over 4 successive periods based upon their readiness. The testing objective is to verify the interoperability of State system functionality, hardware and software, and business logic with the Federal Data Services Hub (FDSH). Testing includes scenarios designed for successful responses as well as unsuccessful but valid responses.
- High level State testing milestones:
 - October 2012: States began informal testing
 - March 2013 - August 2013: Formal "Wave Testing"
 - Mid-July: Start Account Transfer testing between State Medicaid & CHIP Agencies and the Federal Marketplace
 - Mid-July: All States will begin regression testing
 - Mid-August to August 31: All partner End to End testing
- Composition of State testing:
 - Total States Testing with Hub: 46 states (two more States are expected to join testing next week)
 - The 46 States break down into
 - 15 State Based Marketplaces,
 - 13 State Partner Marketplaces, and
 - 18 Federally Facilitated Marketplaces.

- **Results:**
 - Testing progress varies by state, depending on the readiness of the state system. Some states have successfully completed testing on multiple services, while other states are just getting started.
- **Activities for 10/1/13**
 - Complete onboarding and testing of the remaining States
 - Complete Operational Readiness Review (ORR)
 - Receive State tailoring of FFM Modified Adjusted Gross Income (MAGI) rules to support Medicaid eligibility determinations.
 - Determination and approval of advance Cost Sharing Reductions (CSR) estimate required by September 2013
 - Processing of transactional enrollment files (834s) from State Based Marketplaces (SBM) required by October 2013
- **Risks for Day 10/1/13**
 - SBMs are responsible for the readiness of their State Marketplace and CMS cannot support late conversions to the FFM
 - Integrated Medicaid & CHIP eligibility systems may need to utilize FFM if their MAGI eligibility determination functionality is not ready
- **Activities for 1/1/14**
 - States that did not meet Account Transfer readiness by 10/1 will be tested
 - Data exchanges between CMS and SBMs for Federally-administered functions
 - Enrollment reconciliation with SBMs, including Advanced Premium Tax Credit (APTC) and CSR amounts required by December 2013
- **Risks for 1/1/14**
 - States that do not complete their Account Transfer functionality will need to utilize alternate methods for transferring individuals

FEDERAL

- **High level Federal testing milestones:**
 - October 2012: Testing with IRS started
 - Current: CMS is testing with Medicare, IRS, SSA, DHS, Peace Corps and OPM
 - 8/15: Federal Agencies will begin participation in End to End testing on 8/15
- **Activities for Day 1**
 - Initiate (and complete) testing with VHA & TRICARE
 - Onboard Federal Agencies into Production environment
- **Risks for Day 1**
 - VHA & TRICARE not ready for Day 1 affecting Minimal Essential Coverage checks

ISSUERS*Eligibility & Enrollment*

- CMS worked with Issuers to define test scenarios with the emphasis on the ability to perform Qualified Health Plan (QHP) enrollments. Issuer QHP Enrollment Integration Testing consists of FFM-Initiated Enrollment transaction testing as well as optional Issuer Direct Enrollment processing via web services
- **High level Issuer testing milestones:**
 - June 2013: Testing with Issuers began
 - FFM-Initiated Enrollment Testing
 - Week of 7/15: Engage the first wave of 7 Issuers for functional FFM-Initiated Enrollment Testing
 - Early August: Engage the second wave of Issuers with approximately 125 participants.
 - Mid-August: Additional testing waves will be conducted every two weeks for FFM-Initiated Enrollment testing leading up to the October 1st go-live for Open Enrollment.
 - Direct Enrollment Integration Testing
 - Week of 7/22: Direct Enrollment Testing starts for all interested Issuers, and will be ongoing throughout the months of August and September.
- **Results**
 - To date, CMS has received 140 approved Issuer Onboarding Forms, covering 600 QHPs.
 - Thus far, CMS has received 80 applications from Issuers wishing to participate in Direct Enrollment.
 - Hub Partner IDs have been created for 33 Issuers; CMS is awaiting response from the remaining 47 Issuers that have applied.
 - 15 Issuers have demonstrated the ability to connect to Hub services to perform Direct Enrollment.
- **Activities for Day 1**
 - Onboard all Issuers with Marketplace QHP
 - Complete planned Direct Enrollments and FFM -Initiated Enrollment testing with every Issuer
- **Risks for Day 1**
 - Issuers not ready for Day 1 affecting Marketplace QHP enrollments
- **Activities for 1/1/14**
 - After Enrollment Integration Testing, CMS will continue to test new functionality with Issuers, such as Enrollment Reconciliation and EDI Payment Remittance, which are required by January 1, 2014.
 - First payment due to Issuers required by January 2014
 - Commence issuer edge server processing for claims/enrollee data required by January 2014

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Saturday, July 13, 2013 10:05 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Bowen, Marianne (CMS/OA)
Subject: Re: Testing information

Todd Coutts sent me the descriptions of the readiness reviews and we were checking with Marianne to see if she had anything to add, but here it is without Marianne's additions.

CMS is performing a series of IT Readiness Reviews designed to ensure that the Federally Facilitated Marketplace (FFM) IT systems are prepared to support Open Enrollment on October 1 and the beginning of payments in January 2014. The Reviews include all relevant contractor and Federal teams. To ensure that the Reviews cover the multiple aspects of IT readiness, we have organized the reviews into several components.

1. A **functional walkthrough** that focuses on the IT capabilities required to support the actions that a consumer will take to enroll through the Health Insurance Marketplace. These Reviews will inspect the IT capabilities required to facilitate two primary activities: (1) enrolling a consumer into a Qualified Health Plan (QHP) on the FFM or (2) transferring a consumer to a State Medicaid Agency for Medicaid/CHIP enrollment. IT capabilities include Healthcare.gov website functionality, eligibility determinations based on Federal data sources (transmitted via the Data Services Hub), etc.
2. The **IT processes and infrastructure** reviews will examine the following four elements of the FFM IT systems:
 - **Security** - The IT security review will ensure that the systems include the proper Federal security and privacy controls to protect sensitive data (e.g. FISMA, HIPAA, etc);
 - **Operations** - The IT operations review will verify that the necessary human and technical resources will be prepared to run the systems on a daily basis. We will include a review of the help desk operations required to provide effective and efficient customer service for consumers and other business partners;
 - **Infrastructure** - The infrastructure portion of the review will focus on the hardware, software, and network capacity of the FFM IT systems. The goal of the infrastructure review is to ensure the availability and performance of the systems; and
 - **Tactical Deployment** - Finally, we will review the plan for the "go-live" event. This review will walk through the checklists and tasks to "turn on" the system to make it available to the public and finalize the connections to Federal and State partners.
3. The **external partner** review will focus on the interaction with the FFM's business partners: i.e. Issuers, States, and Federal Agencies. We will assess the status of agreements with each partner, the readiness of each external partner to engage in IT interactions with the Marketplace, and the plan for coordinated business and IT operations.

Each review includes a detailed assessment of status and results in an actionable follow up plan to address risks and focus our implementation efforts and resources.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Todd Park <[REDACTED]>
Date: Sun, 14 Jul 2013 01:03:31 +0000
To: HENRY CHAO <[REDACTED]>
Cc: Michelle Snyder <[REDACTED]>
Subject: Re: Testing information

Henry, thanks so much, will read this tonight! I think you were also going to send the 9 questions + a couple of bullets describing (at a high level) the readiness review process?

Thanks! Will send you and Michelle a draft document tomorrow.

Cheers,
Todd

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, July 13, 2013 08:44 PM
To: Park, Todd
Cc: Snyder, Michele (CMS/OA) <[REDACTED]>
Subject: Testing information

Attached is the requested information you asked for on testing.

Let me know if you need anything else.

Thanks

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Chao, Henry (CMS/OIS) - [REDACTED]
Sent: Monday, July 15, 2013 2:12 PM
To: Snyder, Michelle (CMS/OA); Park, Todd
Subject: RE: Draft write-up
Attachments: DRAFT summary write-up with Henry Changes.docx
Importance: High

Here are my changes

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Snyder, Michelle (CMS/OA)
Sent: Monday, July 15, 2013 1:54 PM
To: Todd Y Park [REDACTED]; Chao, Henry (CMS/OIS)
Subject: Re: Draft write-up

Looks good

Readiness reviews will continue throughout december as functions evolve and change. Henry is figuring out frequency by function so defer to him

Also - the 9th question on SHCP needs revisited given recent decisions. We left it on as a placeholder. For your backpocket the 9 questions map to over 90 plus data sources and items. Also - the front end guys - training and consumer assistance is underway and will be eventually subsumed into a management information dashboard

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:[REDACTED]]
Sent: Monday, July 15, 2013 12:02 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Draft write-up

Hi Henry and Michelle, here's the draft write-up for the 4:30 meeting this afternoon. I am keeping it high-level, as you'll see.... Any and all edits would be greatly appreciated! Henry, I'll connect with you at 2:15 pm, thanks!

DRAFT, PRE-DECISIONAL, AND CONFIDENTIAL

MARKETPLACE IT CHECK-IN SUMMARY

- FFM and Hub IT is on track to be up and running for October 1 go-live
 - Need to continue to hold the line with respect to lockdown of business requirements and enforcing that no changes can be made without extreme risk to schedule and delivery by October 1 and **January 1**.
 - Readiness reviews (by Functional areas like Eligibility & Enrollment and Operational areas such as Connectivity & Testing) are being executed nearly every week from now through October 1 and January 1. will enable identification and resolution of issues based on comprehensive walk-throughs
 - Testing of data flows between Hub and the Federal Agencies (IRS, SSA, DHS, VA, OPM, CMS/Medicare, Peace Corps) is far along., Testing is in mid-process with States, and in the early stages with Issuers.
 - o Need for CMS tech/ops leads to interact with Issuer tech/ops leads on a free flowing, on-demand basis to ensure flexibility and responsiveness in focusing on results
 - o End-to-end testing with all partners planned for August 15 to 31
 - Post October 1, development and testing work will continue at high-intensity on additional FFM modules required to support financial management/plan payment to support the beginning of payments to Issuers in Jan 2014
- As with any large-scale new program launch, there will be glitches and issues on and after go-live. CMS has stood up and is in the process of operationalizing a Marketplace Operations Center that will monitor Marketplace operations and systems and lead rapid -responses to issues as they arise. It will be important to ensure that the Center is fully staffed with both dedicated technical and business staff.
 - o As with any new operations at this scale the issues need time for analysis before executing fixes and alternate processes DO NOT PANIC!
- It will be critical to tightly manage the flow and approval of QHP data over the next two months
 - State DOI approval of plans and all data to CMS for validation: 7/31
 - Beginning 8/1: Issuers review plans via Plan Compare view
 - CMS does final QA of plans
 - 9/7: Plans are certified and scheduled to be displayed
- State-Based Marketplaces
 - Important to stick with "pivot" decision-making deadline and clearly communicate to SBMs that they are accountable for bringing their marketplaces live. (FFM will not be able to backfill for

them at the last second). There's no room in the schedule or resources to shift if any part of the "pivot" decision gets reworked, modified, amended, changed, even on a small scale like website changes

- Consumer experience will vary from SBM to SBM based on their individual design decisions and execution completely intended to be in the states' domain
- CMS is prepping the systems capabilities to answer 9 essential FFM questions post-go-live:
 - How many consumer applications?
 - How many consumer eligibility determinations?
 - How many consumer enrollments into QHPs?
 - How much are consumer premiums?
 - How many consumers are receiving financial assistance?
 - How many consumer health plan choices?
 - How are consumers using assistance channels?
 - How are CMS Marketplace operations performing?
 - How many employers and employees are served by SHOP?

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Monday, July 15, 2013 4:28 PM
To: Park, Todd; Snyder, Michelle (CMS/OA)
Subject: RE: Draft write-up

Importance: High

Just caught an important distinction to be made...

-- 9/7: Plans are certified and scheduled to be displayed

I think the "displayed" is internal cross checking and not consumer facing. Consumer facing is 10/1.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Monday, July 15, 2013 4:25 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: RE: Draft write-up

Final version for the 4:30 attached please keep very close hold. I am bringing hard copies only to the 4:30 meeting. Thanks!

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Monday, July 15, 2013 2:12 PM
To: Snyder, Michelle (CMS/OA); Park, Todd
Subject: RE: Draft write-up
Importance: High

Here are my changes

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Snyder, Michelle (CMS/OA)
Sent: Monday, July 15, 2013 1:54 PM

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Tuesday, July 16, 2013 5:53 PM
To: Park, Todd; Tavener, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian
Subject: Re: Two quick things

We are in a hearing tomorrow and will not be able to comment until the afternoon at the earliest.

We need to talk abt attendance at readiness reviews. I am sure you can anticipate my position on that
Flys on the wall are seldom invisible and often distracting!!!!

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, July 16, 2013 05:44 PM
To: Tavener, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian <[REDACTED]>
Subject: Two quick things

Hi Marilyn, Aryana, Michelle, and Henry! Two quick items:

1. I will be working on and sending you draft slides [REDACTED] tonight. They will basically be a Powerpoint-ized version of the Word document we reviewed. If you could get me any comments by noon tomorrow, that would be terrific. I would like at that point to send the slides to Mark/Jeanne for their review.
2. I am very much looking forward to being a fly on the wall at the E&E readiness review on the 19th. I'll be able to attend from 11 am to 4 pm. (a) Is this still happening on the 19th? (b) Will this include a walkthrough of the FFM web workflow, including Plan Compare? The reason I ask is that David Simas is very interested in being a fly on the wall for a walkthrough of the FFM web workflow, and also would love to soak up a sense of the underlying complexity of the overall Mktplace machine. If the 19th will include a walkthrough of the FFM web workflow, then wanted to ask if David could come with me (for some or all of the time). He would really appreciate the opportunity, and/but also doesn't want to disrupt things in any way.... (FYI, I've briefed him in detail about the fact that we've locked down business requirements and are in pure operational execution mode for Oct 1/Jan 1). Thoughts?

Thank you!
Todd

To: Todd Y Park [mailto:]; Chao, Henry (CMS/OIS)
Subject: Re: Draft write-up

Looks good

Readiness reviews will continue throughout december as functions evolve and change. Henry is figuring out frequency by function so defer to him

Also - the 9th question on SHOP needs revisited given recent decisions. We left it on as a placeholder. For your backpocket the 9 questions map to over 90 plus data sources and items. Also - the front end guys - training and consumer assistance is underway and will be eventually subsumed into a management information dashboard

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:]
Sent: Monday, July 15, 2013 12:02 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Draft write-up

Hi Henry and Michelle, here's the draft write-up for the 4:30 meeting this afternoon - am keeping it high-level, as you'll see.... Any and all edits would be greatly appreciated! Henry, I'll connect with you at 2:15 pm, thanks!

From: Park, Todd
Sent: Wednesday, July 17, 2013 12:33 AM
To: 'Michelle.Snyder'; 'Marilyn.Tavener'; 'Aryana.Khalid'; 'henry.chao'
Cc: Graubard, Vivian
Subject: RE: Two quick things
Attachments: IT slide v1.pptx

Hi team, draft slide enclosed (hews closely to the Word document) any edits by 4 pm tomorrow (Wednesday) would be hugely appreciated, thanks!

From: Park, Todd
Sent: Tuesday, July 16, 2013 7:10 PM
To: 'Michelle.Snyder'; 'Marilyn.Tavener'; 'Aryana.Khalid'; 'henry.chao'
Cc: Graubard, Vivian
Subject: Re: Two quick things

OK, no problem – it looks like I only need to put together one slide, and it will adhere tightly to and simply summarize the points in the Word doc. Will send the slide to you tonight – if you could send me any edits by 4 pm tomorrow, that would be great; draft slides are being circulated to Deputies for comment at 5 pm. (It will take you 5 min to read the slide)

And I/ David won't come to the readiness reviews -- don't want to distract or disrupt, which upon reflection I suspect would happen even if we didn't say a single thing.

(Will follow up later about a possible focused briefing session for David and me in Baltimore that happens at the appropriate moment)

May the Force be with you in the hearing tomorrow,

Todd

From: Snyder, Michelle (CMS/OA) [mailto:];
Sent: Tuesday, July 16, 2013 05:53 PM
To: Park, Todd; Tavener, Marilyn (CMS/OA) <>; Khalid, Aryana C. (CMS/OA) <>; Chao, Henry (CMS/OIS) <>
Cc: Graubard, Vivian
Subject: Re: Two quick things

We are in a hearing tomorrow and will not be able to comment until the afternoon at the earliest

We need to talk about attendance at readiness reviews. I am sure you can anticipate my position on that. Flies on the wall are seldom invisible and often distracting!!!!

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:]
Sent: Tuesday, July 16, 2013 05:44 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian < >
Subject: Two quick things

Hi Marilyn, Aryana, Michelle, and Henry! Two quick items:

1. I will be working on and sending you draft slides [redacted] tonight they will basically be a Powerpoint-ized version of the Word document we reviewed. If you could get me any comments by noon tomorrow, that would be terrific. I would like at that point to send the slides to Mark/Jeanne for their review.
2. I am very much looking forward to being a fly on the wall at the E&E readiness review on the 19th. I'll be able to attend from 11 am to 4 pm. (a) Is this still happening on the 19th? (b) Will this include a walkthrough of the FFM web workflow, including Plan Compare? The reason I ask is that David Simas is very interested in being a fly on the wall for a walkthrough of the FFM web workflow, and also would love to soak up a sense of the underlying complexity of the overall Mktplace machine. If the 19th will include a walkthrough of the FFM web workflow, then wanted to ask if David could come with me (for some or all of the time). He would really appreciate the opportunity, and/but also doesn't want to disrupt things in any way.... (FYI, I've briefed him in detail about the fact that we've locked down business requirements and are in pure operational execution mode for Oct 1/Jan 1). Thoughts?

Thank you!
Todd

Marketplace IT Status Summary

- **Federally Facilitated Marketplace and Data Hub IT are on track to be up and running for October 1 go-live**
 - Need to continue to hold the line with respect to lockdown of business requirements
 - Readiness reviews by functional area are being executed nearly every week from now through Oct 1 and Jan 1, enabling identification and resolution of issues
 - Testing of data flows among Federal agencies is far along, is in mid-process with States, and is in the early stages with Issuers. End-to-end testing with all partners is planned for Aug 15-31
 - Post Oct 1, development and testing work will continue at high intensity on additional FFM modules required to support financial mgmt/plan payment beginning Jan 2014
- **As with any large-scale new program launch, there will be a stream of issues on and after go-live – CMS is standing up a Marketplace Operations Center to monitor operations and systems and lead rapid response to issues as they arise**
- **Will be critical to tightly manage the flow and approval of Qualified Health Plan data over the next two months – i.e., State Department of Insurance approval of plans (7/31), Issuer review of their plans via FFM Plan Compare view (beginning 8/1), CMS review, final certification of plans for display (9/7)**
- **State-Based Marketplaces – need SBMs to understand unequivocally that they are accountable for bringing live Marketplaces in their states by Oct 1 (FFM cannot backfill at the last second)**

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Wednesday, July 17, 2013 5:05 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian
Subject: Re: Two quick things

Sorry. Just got off the hill. Slide looks fine. No edits.

Thanks

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, July 17, 2013 12:33 AM
To: Snyder, Michelle (CMS/OA); Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian <[REDACTED]>
Subject: RE: Two quick things

Hi team, draft slide enclosed (hears closely to the Word document) any edits by 4 pm tomorrow (Wednesday) would be hugely appreciated, thanks!

From: Park, Todd
Sent: Tuesday, July 16, 2013 7:10 PM
To: 'Michelle.Snyder [REDACTED]'; 'Marilyn.Tavenner [REDACTED]'; 'Aryana.Khalid [REDACTED]'; 'henry.chao [REDACTED]'
Cc: Graubard, Vivian
Subject: Re: Two quick things

OK, no problem -- it looks like I only need to put together one slide, and it will adhere tightly to and simply summarize the points in the Word doc. Will send the slide to you tonight -- if you could send me any edits by 4 pm tomorrow, that would be great; draft slides are being circulated to Deputies for comment at 5 pm. (It will take you 5 min to read the slide)

And I/ David won't come to the readiness reviews -- don't want to distract or disrupt, which upon reflection I suspect would happen even if we didn't say a single thing.

(Will follow up later about a possible focused briefing session for David and me in Baltimore that happens at the appropriate moment)

May the Force be with you in the hearing tomorrow,

Todd

Exhibit ←

From: Allen, Jessica
Sent: Monday, July 08, 2013 06:01 PM
To: DL-WHO-Press
Subject: NYT: 10 Questions for Obama's Chief Technology Officer

<http://thecaucus.blogs.nytimes.com/2013/07/08/10-questions-for-obamas-chief-technology-officer/?src=twr>

July 8, 2013, 5:48 pm

10 Questions for Obama's Chief Technology Officer

By [JOHN HARWOOD](#)

[VIDEO](#)

Todd Park, a former Silicon Valley entrepreneur, serves as President Obama's chief technology officer. His role has taken on heightened importance after several recent developments, including the implementation of the new health care law, efforts to reduce the backlog in Department of Veterans Affairs claims processing, and privacy issues raised by disclosures about data collection by the National Security Agency. Mr. Park spoke with John Harwood of The Times and CNBC at the White House as Mr. Obama publicly challenged his administration to improve the government's innovation and efficiency in his second term.

What follows is a condensed, edited account of their conversation.

Q.

Government has a reputation for being clunky, slow, inefficient. What do you think you have been able to accomplish?

A.

There are phenomenal people harnessing the power of tech and innovation to help government work better, cost less and help grow the economy. For example, in the recent Hurricane Sandy and Oklahoma tornado response, FEMA has



harnessed tech in all kinds of ways to deliver better results. To get housing to folks, you used to rely exclusively on the ground inspectors, now we can use satellite and analytics to figure out what areas need help and get help faster. In addition, a majority of folks who registered for disaster aid post-Sandy were able to do so via mobile phone or Internet. Even when folks didn't have access, FEMA inspectors came back with iPads to actually register them for aid.

Another example: I was recently traveling with the president to Austin, where he launched a new executive order that opens up tons of government data—everything from health and medicine and science to safety and more—as machine-readable, free fuel for entrepreneurs to tap to create new companies and jobs. The president's attitude is, this is America's data. All kinds of entrepreneurs are picking up that data to help grow the economy.

Q.

Possibly the biggest thing the government has going right now is trying to implement the health care law. The administration announced a delay in the employer mandate; they couldn't get it done in time. What does that tell you about the limits of technology in making it work more rapidly and efficiently?

A.

The president is really focused on implementing the law very well. Business expressed concern that there are issues to be worked through, so it was a sensible thing to do to say, "O.K., let's work through those issues." Oct. 1, we'll be bringing live the new health marketplaces. Things are on track to make that happen. There is a whole team at the U.S. Department of Health and Human Services working incredibly hard, night and day, on bringing out these new health marketplaces. We have actually done a huge amount of user testing on it to make sure the Web site is as user-friendly as possible. The prototypes are incredibly impressive.

Q.

No doubt they'll be up and running in October?

A.

They'll be up and running Oct. 1.

Q.

Let me ask you about the culture of Washington. It has a reputation as being the opposite of the Silicon Valley culture in terms of agility and decision-making, flexibility, innovation. What have you found?

A.

I have actually found a lot more similarities than you might expect. Whenever the president gives us a mission to harness tech innovation and get something done for the American people, in terms of growing the economy and improving health care, we go find the folks across government who have been dreaming about that for a really long time. They're out there, they're incredibly talented innovators. We team them together into what we call a virtual start-up that's running inside the government, to move Silicon Valley speed to get stuff done. When you have the air cover like President Obama, who is deeply passionate about harnessing innovation and tech, it is possible for these focused teams to get a lot done in a short period of time. It's hard to actually build anything new, but it turns out if you apply a lot of the same techniques that make Silicon Valley companies successful to internally change parts of the government, they definitely work.

Q.

Talk about how those virtual start-ups work, and how many are there?

A:

The way they operate is modeled on a philosophy called "lean start-up," which was popularized recently by Eric Ries. You want to build small, interdisciplinary, agile teams that have strategy, policy, ops and tech all represented in one team, all working to solve one problem. Secondly, there's an emphasis on rapid prototype. You don't think aircraft carrier, you think row boat - the smallest possible thing I can deliver to my actual customer as early as possible, so they can actually start getting their engagement. The third principle is rapid iteration - iterate that product at high speeds with versions released every few days or every few weeks, instead of every few months or years, so you maximize the learning. So from the ground up, you eventually get to a real understanding of what the customer wanted and how to create something that delivers that. So that's the model that we've been adopting.

There are about 15 or so that I personally oversee. But this is actually a model that's been done across the government. The key is that we have an idea, we find the three or five people initially that had the idea a long time ago or had a similar idea across the government, put them together in this lean start-up team, liberate them to actually operate, give them the air coverage to do so, and they rock 'n' roll from there.

Q:

One of the innovations the president is going to talk about is something called Blue Button at the Department of Veterans Affairs to help people get their medical records quickly. The department has gotten a reputation for the very slow process of handling disability claims, and it has gotten mocked for stacks of paper records. So why shouldn't the average person say, "Great, Blue Button is fantastic," but you have such a bigger problem than that and you aren't making much headway?"

A:

The backlog issue, as you know, is one that the administration inherited. The administration, on top of that, passed a whole set of rules that expand eligibility and increase the number of claims. There is an unprecedented, governmentwide effort that is pretty amazing to take that problem out, to take the whole backlog problem out - to apply technology and process change. We're actually beginning to see the progress of the backlog beginning to come down at a growing clip, and we think we're going to be able to meet our goals there. The president has made it super clear that this is a top, major priority. There's a huge team, a cross-agency team, a cross-government team that's actually working very hard at this complex problem and taking it out.

Q:

You did consulting for Booz Allen Hamilton, the firm that employed the National Security Agency leaker Edward J. Snowden. What is your concern in regard to privacy with government technology and the centralization of information?

A:

It's incredibly important to protect personal privacy, and it's something that the administration has been championing from the very beginning, advocating for consumer privacy bill of rights and making sure we build privacy protections into the Affordable Care Act and lots of different venues of activity. I think a lot has been accomplished there. I think it's important to stay abreast of the continuing trends, and to make sure that we are tracking with those trends and ensuring that consumer privacy is protected everywhere possible.

Q:

What's a reasonable way of looking at the success of the open-data policy that the president implemented? How quickly will we see results from that?

A:

That's something actually that we've been working on since the president's first day in office, when he submitted his open-government memorandum. There's over 75,000 data sets on data.gov already, everything from daily hospital charges for different procedures across the country, to credit card complaints, account affordability, weather, climate, and so forth. So there's a bunch of data that's already been out there, and a bunch of data that has been downloaded and used by companies like [Opower](http://Opower.com), which is a start-up that uses government energy trends and weather data to help consumers save money on their energy bills. Companies like [Triage](http://Triage.com), which was started a couple of years ago from a couple of emergency room doctors from Denver, that used downloaded data from the Department of Health and Human Services to help you use on a mobile app, based on what's wrong with you, to get the best local doctors and hospitals to help you. What the executive order does is it says, going forward as a new default, all new or modernized government resources should be made open and machine-readable while protecting privacy and national security, which turbocharges the number of data sets on data.gov, and therefore turbocharges the new company creation and job creation that results.

Q.

Do you feel, as a Silicon Valley guy that has started companies, like a fish out of water in Washington?

A.

A lot of people ask me that question, a lot of my friends back home. It's been the most amazing entrepreneurial experience I've ever had. The opportunity you have here to work with teams that are making changes happen at scale is quite extraordinary. The impact you can have is mass times velocity. If you take an opportunity like this, with the scale of opportunity for change that it has, and combine it with the ability to do lean start-up with air cover of the president to make change happen rapidly, that mass times velocity equation is going to have an impact.

Q.

I thought Washington was all mass and no velocity.

A.

It's interesting. It turns out that it can have velocity on innovation ambitions, if you have a president that cares about that.

Transcribed by Katherine L. Kreider

Exhibit 5

From: Wallace, Mary H. (CMS/OC) <[REDACTED]>
Sent: Saturday, June 29, 2013 10:33 AM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Booth, Jon G. (CMS/OC)
Subject: RE: Follow-up

Todd,

Just to follow up on what Henry flagged with IDEO. We can talk about this more, but I think the real concern is to not have contractors trying to interpret what they think you or others from HHS or the White House asked them to do. The biggest help would be for all of you to carry the message that the best thing IDEO (or any contractor) can do is what CMS is asking them to do. In IDEO's case this is Jon Booth's team giving them direction.

We have a lot of contractors supporting this effort and we are working hard to keep them all on the right track to get everything done in time.

Thanks

Mary

From: Park, Todd [REDACTED]
Sent: Saturday, June 29, 2013 9:26 AM
To: Chao, Henry (CMS/OIS)
Cc: Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: Re: Follow-up

Will work on making both of these things happen as you've requested and report back!

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, June 29, 2013 09:07 AM
To: Park, Todd
Cc: Wallace, Mary H. (CMS/OC) <[REDACTED]>; Booth, Jon G. (CMS/OC) <[REDACTED]>
Subject: Re: Follow-up

Todd,

I talked to Michelle and she would like for the follow-up to just be with you.

Also I wanted to talk to you about a meeting you had with Ideo. Apparently something was misinterpreted from what you said and the top dog you met with circled back to OC (since they are one of the contractors in the mix) and started to work on an alternate rendering of the paper form as if they were instructed to follow a different set of requirements. This is a pretty big issue since Ideo does not get to change requirements and scope without it coming from CMS directly. If there's anything you can do to help clear this up we would greatly appreciate it, or rather the program would appreciate it since it will hold the line on confusion and risk.

Thanks.

Henry Chao

Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[Redacted] (Pri)
[Redacted] (Alt)
[Redacted] (BB)

From: Park, Todd [mailto:[Redacted]]
Sent: Thursday, June 27, 2013 12:26 AM
To: Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian <[Redacted]>; VanRoekel, Steven <[Redacted]>;
Lynch, Laura <[Redacted]>
Subject: RE: Follow-up

Hi Henry, I'd love to try Tuesday, July 9, 4 pm to 8 pm+. Looping Steve and Laura Steve would like to come, too! (Steve, this is the Marketplace IT and testing deep-dive we discussed). Steve, can you make this time?

Viv, if Steve can make this time, let's book it. We should also invite Bryan Sivak and Frank Baitman, if they would like to attend. I'll bring enough carrots, ginger beer, pita bread, and hummus for everybody ☺

Thanks, Henry!
Todd

From: Chao, Henry (CMS/OIS) [mailto:[Redacted]]
Sent: Wednesday, June 26, 2013 11:16 PM
To: Park, Todd
Cc: Graubard, Vivian
Subject: Re: Follow-up

Todd,

For planning purposes I am blocking the following dates and times. Let me know which works for you. Thanks!

- Monday July 8 5pm to at least 9pm
- Tuesday July 9 4pm to at least 8pm
- Monday July 15 5pm to at least 9pm
- Tuesday July 16 4pm to at least 8pm

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[Redacted] (Pri)
[Redacted] (Alt)
[Redacted] (BB)

From: Park, Todd
Sent: Saturday, June 29, 2013 11:43 AM
To: 'Mary.Wallace' <[REDACTED]>; 'henry.chao' <[REDACTED]>
Cc: 'Jon.Booth' <[REDACTED]>
Subject: Re: Follow-up

Hi Mary, thank you for the flag, will absolutely do!

From: Wallace, Mary H. (CMS/OC) [mailto:[REDACTED]]
Sent: Saturday, June 29, 2013 10:33 AM
To: Park, Todd; Chao, Henry (CMS/OIS) <[REDACTED]>
Cc: Booth, Jon G. (CMS/OC) <[REDACTED]>
Subject: RE: Follow-up

Todd,

Just to follow up on what Henry flagged with IDEO. We can talk about this more, but I think the real concern is to not have contractors trying to interpret what they think you or others from HHS or the White House asked them to do. The biggest help would be for all of you to carry the message that the best thing IDEO (or any contractor) can do is what CMS is asking them to do. In IDEO's case this is Jon Booth's team giving them direction.

We have a lot of contractors supporting this effort and we are working hard to keep them all on the right track to get everything done in time.

Thanks

Mary

From: Park, Todd [REDACTED]
Sent: Saturday, June 29, 2013 9:26 AM
To: Chao, Henry (CMS/OIS)
Cc: Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: Re: Follow-up

Will work on making both of these things happen as you've requested and report back!

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, June 29, 2013 09:07 AM
To: Park, Todd
Cc: Wallace, Mary H. (CMS/OC) <[REDACTED]>; Booth, Jon G. (CMS/OC) <[REDACTED]>
Subject: Re: Follow-up

Todd,

I talked to Michelle and she would like for the follow-up to just be with you.

Also I wanted to talk to you about a meeting you had with Ideo. Apparently something was misinterpreted from what you said and the top dog you met with circled back to OC (since they are one of the contractors in the mix) and started to work on an alternate rendering of the paper form as if they were instructed to follow a different set of requirements. This is a pretty big issue since Ideo does not get to change requirements and scope without it coming from CMS directly. If there's anything you can do to help clear this up we would greatly appreciate it, or rather the program would

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Saturday, June 29, 2013 4:32 PM
To: Park, Todd; Wallace, Mary H. (CMS/OC)
Cc: Booth, Jon G. (CMS/OC)
Subject: Re: Follow-up

As soon as Vivian confirms your calendar for the 9th (4pm to?) I was going to send Jon and Mary the appointment.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, June 29, 2013 04:23 PM
To: Wallace, Mary H. (CMS/OC); Chao, Henry (CMS/OIS)
Cc: Booth, Jon G. (CMS/OC)
Subject: Re: Follow-up

Hi team, just pinged Team IDEO (including the CEO) and said that they should be sure to follow CMS's lead, and that CMS is the unambiguous operational leader of all of the Marketplace work, in case that wasn't clear :)

The idea related to UX that came up in the discussion with IDEO's CEO was making sure that ideas to optimize language and UX got the right level of air cover on behalf of the user vs. other policy considerations. We (David Simas and I) expressed support for the idea of ensuring there is a clear process to make UX decisions that are user-centric.

But what I've clarified in our follow-up ping is that we are going to circle back with CMS on this (to understand current UX decisionmaking process and if any further support/air cover for user-centric-ness is needed on an ongoing basis).

And again, I emphasized the need for IDEO to listen to CMS for actual direction :)

Henry, perhaps we can touch base about the UX decisionmaking process at our deep dive? Would be wonderful to have Jon and Mary attend for part of that session to discuss the current state of the UX and ongoing process. If any process optimizations might be useful, they may or may not be relevant for Oct 1, but could be useful post Oct 1.

Please let me know if IDEO remains at all confused about things, and many apologies if we created confusion!

Semper fi,
Todd

EXHIBIT 7

From: Khalid, Aryana C. (CMS/OA) <[REDACTED]>
Sent: Thursday, September 12, 2013 4:06 PM
To: Tavener, Marilyn (CMS/OA); Park, Todd
Cc: Snyder, Michelle (CMS/OA)
Subject: RE: Hi Marilyn

Marilyn is exactly right, we need everyone's support right now and we need folks talking to the advocates saying this is a momentous time in our Country's history, b/c it is. We are standing up something that has never been done before and even though some pieces are coming online a little later, what the team is doing is unprecedented. Not even standing up Medicare and Medicaid can compare to this. We need people out there talking to the advocates and asking them to stand up with us and say this is a big deal and there are many ways for folks to apply:

1. Online in English on day 1
2. With an in-person assister on day 1 in various languages
3. With the call center on day 1 in many languages

I know you are trying to help us and we so appreciate it. What we need is folks focusing on what they can do which is the messaging and talking to the advocates, not focusing on the IT or trying to come up with creative solutions to solve this. I hope this makes sense.

Aryana

From: Tavener, Marilyn (CMS/OA)
Sent: Thursday, September 12, 2013 3:54 PM
To: Todd Y Park [REDACTED]
Cc: Snyder, Michelle (CMS/OA); Khalid, Aryana C. (CMS/OA)
Subject: Re: Hi Marilyn

Yes but go through Michelle first. I am copying her and Aryana. Michelle I had explained to Todd -who was asking gently what the issues were. I told him band width primary so we can not get there by 10/1. Second was implementation risk. Todd I need folks to understand the VERY best way they can help us -is to reach out to the advocates-educate them and garner their energy/support. We have the same issues within Medicaid(meaning functionality coming up in stages)and I have sent Cindy and Andy Schneider to work with advocates. Thanks! M.

From: Park, Todd [mailto:[REDACTED]]
Sent: Thursday, September 12, 2013 03:38 PM
To: Tavener, Marilyn (CMS/OA)
Subject: RE: Hi Marilyn

I know you do :) To help with internal understanding here at the WH (and therefore with mobilizing energy and help for external messaging!), would you mind if I got on the phone with Henry for 5 min to get a quick download on the tech details? It makes a lot of intuitive sense that sequencing would be much safer. It would help if I were armed with a bit more tech detail...

From: Tavener, Marilyn (CMS/OA) [mailto:[REDACTED]]
Sent: Thursday, September 12, 2013 3:30 PM
To: Park, Todd
Subject: Re: Hi Marilyn

And I say it with love:

From: Park, Todd [mailto:]
Sent: Thursday, September 12, 2013 03:13 PM
To: Tavenner, Marilyn (CMS/OA)
Subject: Hi Marilyn

Hi Marilyn, hope all is terrific with you as we enter the home stretch on the road to October 11 everyone's hearts and spirits are with you and team!

I understand that you and Chris had a conversation about HC.gov in Spanish in which you underlined the importance of a smooth go-live on October 1 and therefore the need to push HC.gov in Spanish to Oct 15.

Just to emphasize, Chris is supportive of your position, and did not ask me to ping you!

Macon pinged me, and asked what the root of the technical issue was and if a creative solution might be possible. I said that I would check with you @ Might you be able to circle back with your tech team on this question? If it would be even remotely helpful, I would be more than happy to join the technical conversation as well.

Thank you and team so very much again for the truly heroic work you are doing. may the Force continue to be with you!

Todd

Exhibit 5

From: McGuinness, Tara
 Sent: Saturday, June 22, 2013 10:24 PM
 To: 'Julie.Bataille'; Bryan.Sivak; Park, Todd; Simas, David M.; Lee, Jesse C.
 Subject: Re: this is great.

Also david, maybe when you and todd are in CA this week, you could do some in-person press meetings.

From: Bataille, Julie (CMS/OC) [mailto:];
 Sent: Saturday, June 22, 2013 10:14 PM
 To: McGuinness, Tara; Sivak, Bryan (HHS/IOS) <>; Park, Todd; Simas, David M.; Lee, Jesse C.
 Subject: RE: this is great

There is a blog by Bryan in the works along these lines (Bryan I haven't seen latest version) but assume that could go into an email relatively quickly too --would think we want that timed to code availability, we reference the site in the press release itself. Bryan can make these points at the in person press briefing Monday but since those are really healthcare reporters other calls on these points is probably best to get this story out -am hoping the tech pieces of this will serve as some validation for moving in the right consumer direction as am worried the healthcare folks are likely to be disappointed that the application and plan compare aren't yet live. Let me know what we can do to help.
 Julie

From: McGuinness, Tara [mailto:];
 Sent: Saturday, June 22, 2013 10:05 PM
 To: Sivak, Bryan (HHS/IOS); Park, Todd; Simas, David M.; Bataille, Julie (CMS/ OC); Lee, Jesse C.
 Subject: Re: this is great

+Julie and Jesse

In addition to a tech press push and some mainstream folks who like to write about this, we should have an email drafted (Bryan can you do that) that lays out what we are doing and hyperlinks to more interesting parts of the site and to this piece- this could go to tech elites on Monday. I have some ideas about a list of folks who should receive such an email, but you all might have more.

Todd, do you have a list like that? I am on a techie-organizer google group. I can also check with OPE. I might actually be better coming from an outside validator that us.

--Tara

From: Sivak, Bryan (HHS/IOS) [mailto:];
 Sent: Saturday, June 22, 2013 07:51 PM
 To: Park, Todd; McGuinness, Tara; Simas, David M.
 Subject: Re: this is great

Oh, one other thing: Todd is exactly right -- this is the launch of the the "learn" side, which is the informational, "get prepared" content. The actual marketplace launches (obviously) October 1st, although there will be more functionality added to hc.gov in the interim, such as the ability to create accounts.

On Jun 22, 2013, at 19:14, "Sivak, Bryan (HHS/IOS)" <> wrote:

Longish story. Alex has been following this since we made the design decisions he describes, roughly six months ago. As I think you guys know, we're in "soft launch" mode this weekend and are encouraging people to hold off on Monday to really "break" the news. Having said that, it's the internet and once something is out there, it's out there.

IMHO, Alex put together a really fantastic piece on the technical side of what we're doing. He nailed the importance not just for hc.gov but for gov't tech in a broader sense. I know he's shopping this piece right now and he told me it might get picked up by one or two larger publications.

There are a few other tech details we're holding back until Monday (for example, the <http://www.healthcare.gov/developers> page), which I'm planning on talking to a few other outlets on Monday about once we're in official launch mode. I assume you guys have connections at fairly high levels, so if you want to put me in touch with people, I'm happy to talk today/tomorrow for a Monday publication, or on Monday whenever.

To answer the specific question about code and availability -- we are going to publish the code this week (maybe Monday along with the official launch if everything works out). If you take a look at the [/developers](http://www.healthcare.gov/developers) page you'll see that we have detailed the programmatic mechanisms for accessing content, but have a "coming soon" where the links to the Github repos are.

Happy to answer any other questions. This is a paradigm shift for the federal government and the fact that it's happening on healthcare.gov is a really big deal for the tech community.

Bryan

From: Park, Todd [REDACTED]
Sent: Saturday, June 22, 2013 7:01 PM
To: McGuinness, Tara; Simas, David M.
Cc: Sivak, Bryan (HHS/IOS)
Subject: Re: this is great

Looping Bryan -- I believe what Alex Howard is discussing in this (great) piece is the new HealthCare.gov content site, which is up and running, and for which the code has been posted on Github (an online repository for open source code). The content site will front-end the Marketplace -- but the actual Marketplace eligibility-checking/enrollment/plan compare functionality is not up yet. Bryan, can you confirm/elaborate? Thanks!

Todd

From: McGuinness, Tara
Sent: Saturday, June 22, 2013 06:08 PM
To: Simas, David M.; Park, Todd
Subject: Re: this is great

Yes. Good idea. Interesting -- they found this up. No other reporters have found it. I'll connect w. Folks about a push. Todd, I thought all the code was going up later, not now, am I wrong about that?

From: Simas, David M.
Sent: Saturday, June 22, 2013 04:39 PM
To: McGuinness, Tara; Park, Todd
Subject: this is great

Would be good if other tech related pubs write something good about this.

From: Bataille, Julie (CMS/OC) <julie.bataille@cms.gov>
Sent: Saturday, June 22, 2013 10:14 PM
To: McGuinness, Tara; Sivak, Bryan (HHS/IOS); Park, Todd; Simas, David M.; Lee, Jesse C.
Subject: RE: this is great

There is a blog by Bryan in the works along these lines (Bryan I haven't seen latest version) but assume that could go into an email relatively quickly too --would think we want that timed to code availability, we reference the site in the press release itself. Bryan can make these points at the in person press briefing Monday but since those are really healthcare reporters other calls on these points is probably best to get this story out -am hoping the tech pieces of this will serve as some validation for moving in the right consumer direction as am worried the healthcare folks are likely to be disappointed that the application and plan compare aren't yet live. Let me know what we can do to help.
 Julie

From: McGuinness, Tara [Tara D McGuinness@cms.gov]
Sent: Saturday, June 22, 2013 10:05 PM
To: Sivak, Bryan (HHS/IOS); Park, Todd; Simas, David M.; Bataille, Julie (CMS/OC); Lee, Jesse C.
Subject: Re: this is great

-julie and jesse

In addition to a tech press push and some mainstream folks who like to write about this, we should have an email drafted (bryan can you do that) that lays out what we are doing and hyperlinks to more interesting parts of the site and to this piece- this could go to tech elites on monday. I have some ideas about a list of folks who should receive such an email, but you all might have more.

Todd, do you have a list like that? I am on a techie -organizer google group. I can also check with OP E. I might actually be better coming from an outside validator that us.

-tara

From: Sivak, Bryan (HHS/IOS) [mailto:bryan.sivak@hhs.gov]
Sent: Saturday, June 22, 2013 07:51 PM
To: Park, Todd; McGuinness, Tara; Simas, David M.
Subject: Re: this is great

Oh, one other thing: Todd is exactly right - this is the launch of the the "learn" side, which is the informational, "get prepared" content. The actual marketplace launches (obviously) October 1st, although there will be more functionality added to hc.gov in the interim, such as the ability to create accounts.

On Jun 22, 2013, at 19:14, "Sivak, Bryan (HHS/IOS)" <bryan.sivak@hhs.gov> wrote:

Longish story. Alex has been following this since we made the design decisions he describes, roughly six months ago. As I think you guys know, we're in "soft launch" mode this weekend and are encouraging people to hold off on Monday to really "break" the news. Having said that, it's the internet and once something is out there, it's out there.

IMHO, Alex put together a really fantastic piece on the technical side of what we're doing. He nailed the importance not just for hc.gov but for gov't tech in a broader sense. I know he's shopping this piece right now and he told me it might get picked up by one or two larger publications.

There are a few other tech details we're holding back until Monday (for example, the <http://www.healthcare.gov/developers> page), which I'm planning on talking to a few other outlets on Monday about once we're in official launch mode. I assume you guys have connections at fairly high levels, so if you want to put me in touch with people, I'm happy to talk today/tomorrow for a Monday publication, or on Monday whenever.

To answer the specific question about code and availability -- we are going to publish the code this week (maybe Monday along with the official launch if everything works out). If you take a look at the /developers page you'll see that we have detailed the programmatic mechanisms for accessing content, but have a "coming soon" where the links to the GitHub repos are.

Happy to answer any other questions. This is a paradigm shift for the federal government and the fact that it's happening on [healthcare.gov](http://www.healthcare.gov) is a really big deal for the tech community.

Bryan

From: Park, Todd [REDACTED]
Sent: Saturday, June 22, 2013 7:01 PM
To: McGuinness, Tara; Simas, David M.
Cc: Sivak, Bryan (HHS/IOS)
Subject: Re: this is great

Looping Bryan -- I believe what Alex Howard is discussing in this (great) piece is the new [HealthCare.gov](http://www.HealthCare.gov) content site, which is up and running, and for which the code has been posted on Git hub (an online repository for open source code). The content site will front-end the Marketplace -- but the actual Marketplace eligibility-checking/enrollment/plan compare functionality is not up yet. Bryan, can you confirm/elaborate? Thanks!

Todd

From: McGuinness, Tara
Sent: Saturday, June 22, 2013 06:08 PM
To: Simas, David M.; Park, Todd
Subject: Re: this is great

[REDACTED]

From: Simas, David M.
Sent: Saturday, June 22, 2013 04:39 PM
To: McGuinness, Tara; Park, Todd
Subject: this is great

[REDACTED]

From: Sivak, Bryan (HHS/IOS) <[REDACTED]>
Sent: Saturday, June 22, 2013 11:28 PM
To: Bataille, Julie (CMS/OC); McGuinness, Tara; Park, Todd; Simas, David M.; Lee, Jesse C.
Subject: RE: this is great
Attachments: launchblogdraft-acCS06212013 - bds-aq.docx

Here's the latest version of the blog post. Veronica Jackson in ASPA has it and is planning on sending it out through the regular HHS clearance process next week -- the thought was to do the currently planned campaign with traditional press on Monday (and Tuesday for the Spanish site) and then a day or two later drop this for an additional press hit. Just FYI, there are a couple of things that will probably change slightly with the attached (I think we have better pics of the design team, as an example) but the majority of the content and the structure will remain the same.

I'm happy to work this into an email format for tech elites if you guys want to send something out on Monday. Tara, I know most of the people on that Google group pretty well and can connect directly with them, but keep in mind they're primarily going to be social media amplifiers as opposed to traditional media or web publications.

I was planning on reaching out to some of the tech world publications (TechCrunch, GigaOm, Wired, etc) on Monday post-launch to pitch the story. Happy to coordinate with any other outreach, though.

Todd, David -- let me know who you are going to see in CA, if anyone, and what detail is you need. Some of the usual suspects will already have some info but maybe it's worth hopping on a quick call to discuss.

Bryan

From: Bataille, Julie (CMS/OC)
Sent: Saturday, June 22, 2013 10:14 PM
To: McGuinness, Tara; Sivak, Bryan (HHS/IOS); Park, Todd; Simas, David M.; Lee, Jesse C.
Subject: RE: this is great

There is a blog by Bryan in the works along these lines (Bryan I haven't seen latest version) but assume that could go into an email relatively quickly too -- would think we want that timed to code availability, we reference the site in the press release itself. Bryan can make these points at the in person press briefing Monday but since those are really healthcare reporters other calls on these points is probably best to get this story out. am hoping the tech pieces of this will serve as some validation for moving in the right consumer direction as am worried the healthcare folks are likely to be disappointed that the application and plan compare aren't yet live. Let me know what we can do to help.
 Julie

From: McGuinness, Tara <[REDACTED]>
Sent: Saturday, June 22, 2013 10:05 PM
To: Sivak, Bryan (HHS/IOS); Park, Todd; Simas, David M.; Bataille, Julie (CMS/OC); Lee, Jesse C.
Subject: Re: this is great

+julie and jesse

In addition to a tech press push and some mainstream folks who like to write about this, we should have an email drafted (bryan can you do that) that lays out what we are doing and hyperlinks to more interesting parts of the site and to this piece--this could go to tech elites on Monday. I have some ideas about a list of folks who should receive such an email, but you all might have more.

Todd, do you have a list like that? I am on a techie-organizer google group. I can also check with OPE. I might actually be better coming from an outside validator than us.

<http://e-pluribusunum.com/2013/06/22/why-the-way-the-healthcare-gov-exchange-was-built-matters/>

From: Sivak, Bryan (HHS/IOS) <[REDACTED]>
Sent: Monday, July 01, 2013 1:56 PM
To: Snyder, Michelle (CMS/OA)
Cc: Bataille, Julie (CMS/OC); Chao, Henry (CMS/OIS); Booth, Jon G. (CMS/OC); Wallace, Mary H. (CMS/OC); Herron, Julia (OS/IOS); Trenkle, Tony (CMS/OIS); Patel, Ketan (CMS/OC); Park, Todd; Baitman, Frank (OS/ASA/OCIO); Monteleone, Timothy (OS/ASA); Bowen, Marianne (CMS/OA); Armstead, Andrea E. (CMS/OA); Kerr, James T. (CMS/CMHPO); Khalid, Aryana C. (CMS/OA); Boulanger, Jennifer L. (CMS)
Subject: Re: HealthCare.gov Open Source Release

I am more than happy to be point on this for any inquires from the Hill. Feel free to send them my way.

Bryan

On Jul 1, 2013, at 15:42, "Snyder, Michelle (CMS/OA)" <[REDACTED]> wrote:

We are getting lots of questions about privacy, program integrity etc from the Hill. We need some c's and a's on this....believe me the questions will be asked. If there had been a broad discussion about this I doubt that we would have agreed to impleme nt quite this way. Who owns the story line on this? Copied Jennifer OL needs to be in the loop going forward given all the activity on the HUB and Marketplace front.

Michelle

A.Michelle Snyder
 Chief Operating Officer
 DHHS/CMS/OA
 [REDACTED]

From: Bataille, Julie (CMS/OC)
Sent: Saturday, June 29, 2013 7:19 AM
To: Chao, Henry (CMS/OIS); Booth, Jon G. (CMS/OC); Sivak, Bryan (HHS/IOS)
Cc: Wallace, Mary H. (CMS/OC); Herron, Julia (OS/IOS); Trenkle, Tony (CMS/OIS); Patel, Ketan (CMS/OC); Todd Y. Park [REDACTED]; Baitman, Frank (OS/ASA/OCIO); Monteleone, Timothy (OS/ASA); Bowen, Marianne (CMS/OA); Snyder, Michelle (CMS/OA); Armstead, Andrea E. (CMS/OA); Kerr, James T. (CMS/CMHPO); Khalid, Aryana C. (CMS/OA)
Subject: Re: HealthCare.gov Open Source Release

Henry, We share the concerns and are trying to balance many interests as well. We are excited to be at this point. We should put this on the agenda for marilyn's ops meeting as well I think and have added aryana as well.

From: Chao, Henry (CMS/OIS)
Sent: Friday, June 28, 2013 10:11 PM
To: Booth, Jon G. (CMS/OC); Sivak, Bryan (HHS/IOS); Bataille, Julie (CMS/OC)
Cc: Wallace, Mary H. (CMS/OC); Herron, Julia (OS/IOS); Trenkle, Tony (CMS/OIS); Patel, Ketan (CMS/OC); Todd Y. Park [REDACTED]; Baitman, Frank (OS/ASA/OCIO); Monteleone, Timothy (OS/ASA); Bowen, Marianne (CMS/OA); Snyder, Michelle (CMS/OA); Armstead, Andrea E. (CMS/OA); Kerr, James T. (CMS/CMHPO)

Subject: Re: [HealthCare.gov](#) Open Source Release

I want to express my reservations about putting nearly all the source code for the [hc.gov/Marketplace](#) Portal Website on Github and making it available for absolutely anyone in the entire world to use. While in its current state it does not contain the code for the Online Application, someone with less than honorable intentions can easily stand up a shadow site that would fake out the general public and they can do it easily and literally in just a day or less.

While I believe and support sharing and being open about our codebase I think we have to balance that with safeguarding security, privacy, and the public trust.

I understand OC was told to do this so I am not challenging that. What I am going to advocate though is that we draw the line here and at our next release on 7/15, which contains the beginnings of "MyAccount" where people can start submitting their PHI that CMS will not be putting that entire codebase out for anyone to use. We can work on doing it in such a way that it makes it difficult for anyone to stand up a shadow/phony site if necessary.

I've copied Frank, Todd, and Michelle to make sure they are aware of this and my position.

Thanks,

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

 (Pri)
(Alt)
(BB)

From: Booth, Jon G. (CMS/OC)
Sent: Friday, June 28, 2013 08:25 PM
To: Sivak, Bryan (HHS/IOS); Bataille, Julie (CMS/OC)
Cc: Wallace, Mary H. (CMS/OC); Herron, Julia (OS/IOS); Chao, Henry (CMS/OIS); Trenkle, Tony (CMS/OIS); Patel, Ketan (CMS/OC)
Subject: [HealthCare.gov](#) Open Source Release

Bryan & Julie,

I wanted to let you know that the [HealthCare.gov](#) open source release is now live (in conjunction with the 1.1 release that we just pushed to production).

The Developers page (<https://www.healthcare.gov/developers>) has been updated with a link to our GitHub repo, which is located at <https://github.com/CMSgov/HealthCare.gov-Open-Source-Release>.

Please let me know if you have any questions or feedback.

Thanks,

Jon

From: Sivak, Bryan (HHS/OIS) <[REDACTED]>
Sent: Saturday, June 29, 2013 2:09 AM
To: Chao, Henry (CMS/OIS)
Cc: Booth, Jon G. (CMS/OC); Bataille, Julie (CMS/OC); Wallace, Mary H. (CMS/OC); Herron, Julia (OS/OIS); Trenkle, Tony (CMS/OIS); Patel, Kitan (CMS/OC); Park, Todd; Baitman, Frank (OS/ASA/OCIO); Monteleone, Timothy (OS/ASA); Bowen, Marianne (CMS/OA); Snyder, Michelle (CMS/OA); Armstead, Andrea E. (CMS/OA); Kerr, James T. (CMS/CMHPO); Kendall, Damaris (HHS/OIS)
Subject: Re: HealthCare.gov Open Source Release

Henry,

I understand your concerns and am happy to discuss this when I am back from vacation. Damaris can set up some time to talk.

Bryan

On Jun 29, 2013, at 4:11, "Chao, Henry (CMS/OIS)" <[REDACTED]> wrote:

I want to express my reservations about putting nearly all the source code for the hc.gov/Marketplace Portal Website on Github and making it available for absolutely anyone in the entire world to use. While in its current state it does not contain the code for the Online Application, someone with less than honorable intentions can easily stand up a shadow site that would fake out the general public and they can do it easily and literally in just a day or less.

While I believe and support sharing and being open about our codebase I think we have to balance that with safeguarding security, privacy, and the public trust.

I understand OC was told to do this so I am not challenging that. What I am going to advocate though is that we draw the line here and at our next release on 7/15, which contains the beginnings of "MyAccount" where people can start submitting their PII that CMS will not be putting that entire codebase out for anyone to use. We can work on doing it in such a way that it makes it difficult for anyone to stand up a shadow/phony site if necessary.

I've copied Frank, Todd, and Michelle to make sure they are aware of this and my position.

Thanks.

Henry Chao
 Deputy Chief Information Officer and Deputy Director
 Office of Information Services
 Centers for Medicare & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244

[REDACTED]
 (Pri)
 (Alt)

[REDACTED] (BB)

From: Booth, Jon G. (CMS/OC)
Sent: Friday, June 28, 2013 08:25 PM
To: Svak, Bryan (HHS/IOS); Bataille, Julie (CMS/OC)
Cc: Wallace, Mary H. (CMS/OC); Herron, Julia (OS/IOS); Chao, Henry (CMS/OIS); Trenkle, Tony (CMS/OIS); Patel, Ketan (CMS/OC)
Subject: HealthCare.gov Open Source Release

Bryan & Julie,

I wanted to let you know that the HealthCare.gov open source release is now live (in conjunction with the 1.1 release that we just pushed to production).

The Developers page (<https://www.healthcare.gov/developers>) has been updated with a link to our GitHub repo, which is located at <https://github.com/CMSgov/HealthCare.gov-Open-Source-Release>

Please let me know if you have any questions or feedback.

Thanks,

Jon

Exhibit 6

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Tuesday, July 09, 2013 11:18 PM
To: Couts, Todd (CMS/OIS)
Cc: Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Park, Todd; Graubard, Vivian; Berkley, Katrina (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Subject: Sending Todd Park the series of Readiness Walk Through appointments

Todd,

Vivian is Todd Park's scheduler so please send her the appointment for the 7/19 E&E walk through and any other tentative dates for the other reviews. Todd mentioned he might not make it to all but would try to make the 19th and any others that he knows about.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services

7500 Security Blvd
Baltimore, MD 21244

[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Park, Todd
Sent: Wednesday, July 10, 2013 12:56 AM
To: michelle.snyder [REDACTED]
Cc: henry.chao [REDACTED]; Graubard, Vivian
Subject: Getting together

Hi Michelle, spent five great hours this evening with Henry and the rest of your terrific IT team they are doing truly amazing work!

When are you next in DC? Would love to see if we can get together in the next few days or the beginning of next week so that (a) I can run a summary IT status writeup by you, and which I will subsequently review with Marilyn (very high - level slide or two, for presentation at an up coming WH ACA monthly meeting) and (b) we can go over high -level status of action on key red team recommendations.

I think 30 min would be enough time. We can call Henry in. Thoughts?

Thank you!
Todd

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Tuesday, July 16, 2013 6:24 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Cc: Graubard, Vivian; Kerr, James T. (CMS/CMHPO)
Subject: RE: Two quick things

Todd,

The 19th will include a crude integrated application for discussion and internal review and will not have the compare piece up and running (recall the data will not be together and validated for testing until at least 8/15 and that's with a partial set).

My recommendation is that the readiness review in which we conduct is not really conducive for being an observer at this point and we should stick to the briefing format for you at various intervals.

Thanks.

Henry Chao
 Deputy CIO & Deputy Director,
 Office of Information Services
 Centers for Medicare & Medicaid Services
 [REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, July 16, 2013 5:44 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian
Subject: Two quick things

Hi Marilyn, Aryana, Michelle, and Henry! Two quick items:

1. I will be working on and sending you draft slides [REDACTED] tonight they will basically be a Powerpoint-ized version of the Word document we reviewed. If you could get me any comments by noon tomorrow, that would be terrific. I would like at that point to send the slides to Mark/Leanne for their review.
2. I am very much looking forward to being a fly on the wall at the E&E readiness review on the 19th. I'll be able to attend from 11 am to 4 pm. (a) Is this still happening on the 19th? (b) Will this include a walkthrough of the FFM web workflow, including Plan Compare? The reason I ask is that David Simas is very interested in being a fly on the wall for a walkthrough of the FFM web workflow, and also would love to soak up a sense of the underlying complexity of the overall Mktplace machine. If the 19th will include a walkthrough of the FFM web workflow, then wanted to ask if David could come with me (for some or all of the time) he would really appreciate the opportunity, and/but also doesn't want to disrupt things in any way.... (FYI, I've briefed him in detail about the fact that we've locked down business requirements and are in pure operational execution mode for Oct 1/Jan 1). Thoughts?

Thank you!
Todd

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Tuesday, July 16, 2013 5:53 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian
Subject: Re: Two quick things

We are in a hearing tomorrow and will not be able to comment until the afternoon at the earliest

We need to talk abt attendance at readiness reviews. I am sure you can anticipate my position on that
 Flys on the wall are seldom invisible and often distracting!!!!

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, July 16, 2013 05:44 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian <[REDACTED]>
Subject: Two quick things

Hi Marilyn, Aryana, Michelle, and Henry! Two quick items:

1. I will be working on and sending you draft slides [REDACTED] tonight they will basically be a Powerpoint-ized version of the Word document we reviewed. If you could get me any comments by noon tomorrow, that would be terrific I would like at that point to send the slides to Mark/Jeanne for their review
2. I am very much looking forward to being a fly on the wall at the E&E readiness review on the 19th. I'll be able to attend from 11 am to 4 pm. (a) Is this still happening on the 19th? (b) Will this include a walkthrough of the FFM web workflow, including Plan Compare? The reason I ask is that David Simas is very interested in being a fly on the wall for a walkthrough of the FFM web workflow; and also would love to soak up a sense of the underlying complexity of the overall Mktplace machine. If the 19th will include a walkthrough of the FFM web workflow, then wanted to ask if David could come with me (for some or all of the time) he would really appreciate the opportunity, and/but also doesn't want to disrupt things in any way.... (FYI, I've briefed him in detail about the fact that we've locked down business requirements and are in pure operational execution mode for Oct 1/Jan 1). Thoughts?

Thank you!
 Todd

From: Coutts, Todd (CMS/OIS) <[REDACTED]>
Sent: Wednesday, July 10, 2013 6:10 PM
To: Graubard, Vivian; Chao, Henry (CMS/OIS)
Cc: Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Park, Todd; Berkley, Katrina (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Subject: RE: Sending Todd Park the series of Readiness Walk Through appointments

Hi Vivian,

Here are the dates:

1. Friday, July 19 (9 to 4): Readiness Review Part 1
2. Wed, July 24 (9 to 4): Readiness Review Part 2
3. Friday, August 2 (8:30 to 3): Readiness Review Part 3

Todd Coutts
Centers for Medicare & Medicaid Services
Office of Info, Services | Consumer Info, & Insurance Systems Group
[REDACTED] (office) | [REDACTED] (mobile) | [REDACTED]
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

-----Original Message-----

From: Graubard, Vivian [mailto:[REDACTED]]
Sent: Wednesday, July 10, 2013 11:28 AM
To: Coutts, Todd (CMS/OIS); Chao, Henry (CMS/OIS)
Cc: Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Park, Todd; Berkley, Katrina (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Subject: RE: Sending Todd Park the series of Readiness Walk Through appointments

Thank you, Henry.

Todd, before sending the appointments, if you wouldn't mind sending me a list of dates I need to block off (or reschedule around) - that would be great.

Thanks,
Vivian

-----Original Message-----

From: Coutts, Todd (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, July 10, 2013 8:24 AM
To: Chao, Henry (CMS/OIS)
Cc: Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Park, Todd; Graubard, Vivian; Berkley, Katrina (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Subject: RE: Sending Todd Park the series of Readiness Walk Through appointments

Yes, I will do that.

Todd Coutts

262

I am in DC this Friday and next Monday. I understand Henry is helping with the write-up. Also got a question from Marilyn last night about have we "shut down the red team exercise". I think the red team is pretty much passé at this juncture given our readiness review activity but we can talk about that as well if you wish.

Michelle

Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, July 10, 2013 12:56 AM
To: Snyder, Michelle (CMS/OA)
Cc: Chao, Henry (CMS/OIS); Graubard, Vivian
Subject: Getting together

Hi Michelle, spent five great hours this evening with Henry and the rest of your terrific IT team they are doing truly amazing work!

When are you next in DC? Would love to see if we can get together in the next few days or the beginning of next week so that (a) I can run a summary IT status writeup by you, and which I will subsequently review with Marilyn (very high-level slide or two, for presentation at an upcoming WH ACA monthly meeting) and (b) we can go over high-level status of action on key red team recommendations.

I think 30 min would be enough time. We can call Henry in. Thoughts?

Thank you!
Todd

From: Park, Todd
Sent: Wednesday, July 17, 2013 12:33 AM
To: 'Michelle.Snyder [mailto: [REDACTED]]; Marilyn.Tavener [mailto: [REDACTED]]; Aryana.Khalid [mailto: [REDACTED]]; henry.chao [mailto: [REDACTED]]
Cc: Graubard, Vivian
Subject: RE: Two quick things
Attachments: IT slide v1.pptx

Hi team, draft slide enclosed (heeds closely to the Word document) any edits by 4 pm tomorrow (Wednesday) would be hugely appreciated, thanks!

From: Park, Todd
Sent: Tuesday, July 16, 2013 7:10 PM
To: 'Michelle.Snyder [mailto: [REDACTED]]; Marilyn.Tavener [mailto: [REDACTED]]; 'Aryana.Khalid [mailto: [REDACTED]]; 'henry.chao [mailto: [REDACTED]]
Cc: Graubard, Vivian
Subject: Re: Two quick things

OK, no problem -- it looks like I only need to put together one slide, and it will adhere tightly to and simply summarize the points in the Word doc. Will send the slide to you tonight -- if you could send me any edits by 4 pm tomorrow, that would be great; draft slides are being circulated to Deputies for comment at 5 pm. (It will take you 5 min to read the slide)

And I/David won't come to the readiness reviews -- don't want to distract or disrupt, which upon reflection I suspect would happen even if we didn't say a single thing.

(Will follow up later about a possible focused briefing session for David and me in Baltimore that happens at the appropriate moment)

May the Force be with you in the hearing tomorrow,

Todd

From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]
Sent: Tuesday, July 16, 2013 05:53 PM
To: Park, Todd; Tavener, Marilyn (CMS/OA) < [REDACTED] >; Khalid, Aryana C. (CMS/OA) < [REDACTED] >; Chao, Henry (CMS/OIS) < [REDACTED] >
Cc: Graubard, Vivian
Subject: Re: Two quick things

We are in a hearing tomorrow and will not be able to comment until the afternoon at the earliest

We need to talk about attendance at readiness reviews. I am sure you can anticipate my position on that. Flies on the wall are seldom invisible and often distracting!!!!

Michelle

Exhibit 7

Sent: Thursday, July 25, 2013 09:53 AM

To: Park, Todd
 Cc: Oh, Mark U. (CMS/OIS) <[redacted]>; Courts, Todd (CMS/OIS) <[redacted]>; Outerbridge, Monique (CMS/OIS) <[redacted]>; Grothe, Kirk A. (CMS/OIS) <[redacted]>; Berkley, Katrina (CMS/OIS) <[redacted]>; Rhones, Rhonda D. (CMS/OIS) <[redacted]>; Graubard, Vivian; rich.martin <rich.martin@[redacted]>; cheryl.campbell <cheryl.campbell@[redacted]>; Lakshmi.Manambedu <Lakshmi.Manambedu@[redacted]>; Mark.Calem <Mark.Calem@[redacted]>; Paul.Weiss <Paul.Weiss@[redacted]>; Wallace, Mary H. (CMS/OC) <[redacted]>; Booth, Jon G. (CMS/OC) <[redacted]>

Subject: Walk through of the online application in hc.gov

Todd,

If you recall we had agreed to provide you a walk through and demo of the online application in its current form so you can get a chance to peek under the covers of hc.gov.

Michelle mentioned you contacted her about this and that I should follow-up with you to schedule the walk through.

Katrina can work with Vivian to find a window of opportunity next week if you agree.

Let us know.

Thanks.

Henry Chao
 Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244
 (Pri)
 (Alt)
 (BB)

From: Mielke, Dawn M.
Sent: Wednesday, July 31, 2013 9:22 AM
To: Snyder, Michelle (CMS/OA); Park, Todd
Cc: Graubard, Vivian
Subject: RE: Walk through of the online application in hc.gov

Sounds good, please call Todd at [REDACTED]

Best regards,
Dawn Mielke

[REDACTED]
Office of Science and Technology Policy
Office: [REDACTED]
Cell: [REDACTED]

-----Original Message-----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]
Sent: Wednesday, July 31, 2013 9:16 AM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian; Mielke, Dawn M.
Subject: RE: Walk through of the online application in hc.gov

How about 9:45..have a number you want me to call on?

michelle

A. Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

-----Original Message-----

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, July 31, 2013 8:32 AM
To: Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian; Mielke, Dawn M.
Subject: Re: Walk through of the online application in hc.gov

Hi Michelle, great -- Henry, please let me know if Aug 5 works for the mtg below; if so, I'll coordinate with Julian and David Simas to try to make sure that we can do 1 visit with all of us, for the sake of time efficiency for you and team.

And Michelle, would love to chat! I can talk anytime between 9:30 and 10:30, at 4:45, or at or any time after 5 pm -- do any of those times work for you?

Cheers,
Todd

----- Original Message -----

From: Park, Todd [mailto: [REDACTED]]
 Sent: Tuesday, July 30, 2013 09:43 PM
 To: Chao, Henry (CMS/OIS)
 Cc: Snyder, Michelle (CMS/OA)
 Subject: RE: Walk through of the online application in hc.gov

Hi Henry and Michelle, just circling back on the below, to see what general date range you think might make sense for this visit -- would next week work? Just need to have a bit of advance time to line up Julian and David's schedules (and I'm out the week of August 12-16). Also: if you want to cut down on the time of the visit, ratcheting it down to something more like 60-90 minutes, or modify the agenda in any way, just let me know....

Thoughts? Thanks!
 Todd

----- Original Message -----

From: Park, Todd
 Sent: Thursday, July 25, 2013 3:01 PM
 To: 'henry.chao [REDACTED]';
 Cc: 'Michelle.Snyder [REDACTED]';
 Subject: Re: Walk through of the online application in hc.gov

Hi Henry, thanks so much! To provide more context, as I shared with Michelle, I'll be bringing David Simas and Julian Harris (Keith Fontenot's successor, newly arrived) with me. Would love to (1) walk through the current live online workflow (ideally from the start of the application through Plan Compare and selection) and (2) provide the opportunity for Julian to get the latest update on (a) IT dev, (b) testing, and (c) operational prep.

For (2), Julian is interested in one level of detail below the [REDACTED] presentation. I would not prepare any custom materials whatsoever for the meeting, but it would be great to show him (a) the slide you showed me with all of the IT modules/completion dates, (b) the testing summary for fed agencies, states, issuers you wrote up recently (I think for someone's testimony), or similar material, and (c) a slide (if you have it) of key operationalization steps (high level) on the road to Oct 1 and Dec 1 (e.g., contract X let, center X live, etc.).

Both Julian and David took great pains to ask that the visit not be disruptive to your work -- I think that the message to give y'all the space to rock and roll is spreading :)

So I'm thinking a focused two-hour visit, in Baltimore, going thru the live workflow, and using high-level materials you already have.

Would next week be best, or would the week after be better, or would either week be fine? I haven't yet pinged David and Julian for their availability, but wanted to see what was optimal for you first. It would be good to combine both of their visits, to save you time. Thoughts on timing?

Michelle, it would be terrific for you to join -- would be great for you to meet Julian and David, both of whom are terrific, and I've told both of them that you and Henry are pure awesomeness :)

Thanks!
 Todd

----- Original Message -----

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Wednesday, July 31, 2013 9:16 AM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian; Mielke, Dawn M.
Subject: RE: Walk through of the online application in hc.gov

How about 9:45..have a number you want me to call on?

michelle

A.Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

-----Original Message-----

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, July 31, 2013 8:32 AM
To: Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Graubard, Vivian; Mielke, Dawn M.
Subject: Re: Walk through of the online application in hc.gov

Hi Michelle, great -- Henry, please let me know if Aug 5 works for the mtg below; if so, I'll coordinate with Julian and David Simas to try to make sure that we can do 1 visit with all of us, for the sake of time efficiency for you and team.

And Michelle, would love to chat! I can talk anytime between 9:30 and 10:30, at 4:45, or at or any time after 6 pm -- do any of those times work for you?

Cheers,
Todd

-----Original Message-----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]
Sent: Wednesday, July 31, 2013 07:48 AM
To: Park, Todd; Chao, Henry (CMS/OIS) <[REDACTED]>
Subject: Re: Walk through of the online application in hc.gov

I think Julian was looking to be here on the 5th. Haven't spoken with Henry as to whether or not that works

Also - Todd - is there a good time to call you today - I have a proposition for you that doesn't involve marketplaces for a change!!!!

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd
Sent: Wednesday, July 31, 2013 9:43 PM
To: 'henry.chao'; 'Michelle.Snyder';
Cc: Graubard, Vivian; Mielke, Dawn M.; monique.outerbridge; Todd.Couts1
Subject: Re: Walk through of the online application in hc.gov

Henry, absolutely no problem, and again, please don't hesitate to say that another day would work better -- we want to prioritize your operational imperatives above all other things!

----- Original Message -----

From: Chao, Henry (CMS/OIS) [mailto:];
Sent: Wednesday, July 31, 2013 08:13 PM
To: Park, Todd; Snyder, Michelle (CMS/OA) < >;
Cc: Graubard, Vivian; Mielke, Dawn M.; Outerbridge, Monique (CMS/OIS) < >; Coutts, Todd (CMS/OIS) < >;
Subject: Re: Walk through of the online application in hc.gov

I have asked the folks involved on the CMS and CGI sides if the 5th will work but it might take until tomorrow to confirm since it is the same people trying to get Lite Account launched.

Will respond as early as possible tomorrow morning.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[Redacted]

On 7/31/13 8:31 AM, "Park, Todd" < > wrote:

>Hi Michelle, great -- Henry, please let me know if Aug 5 works for the
>mtg below; if so, I'll coordinate with Julian and David Simas to try to
>make sure that we can do 1 visit with all of us; for the sake of time
>efficiency for you and team.
>
>And Michelle, would love to chat! I can talk anytime between 9:30 and
>10:30, at 4-4:5, or at or any time after 6 pm -- do any of those times
>work for you?
>
>Cheers,

>Todd

>

>

>----- Original Message -----

>From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]

>Sent: Wednesday, July 31, 2013 07:48 AM

>To: Park, Todd; Chao, Henry (CMS/OIS) < [REDACTED]>

>Subject: Re: Walk through of the online application in hc.gov

>

>I think Julian was looking to be here on the 5th. Haven't spoken with

>Henry as to whether or not that works

>

>Also - Todd - is there a good time to call you today - I have a

>propositiin for you that doesn't involve marketplaces for a change!!!!

>

>Michelle

>-----

>Sent from my BlackBerry Wireless Device

>

>

>----- Original Message -----

>From: Park, Todd [mailto: [REDACTED]]

>Sent: Tuesday, July 30, 2013 09:43 PM

>To: Chao, Henry (CMS/OIS)

>Cc: Snyder, Michelle (CMS/OA)

>Subject: RE: Walk through of the online application in hc.gov

>

>Hi Henry and Michelle, just circling back on the below, to see what

>general date range you think might make sense for this visit -- would

>next week work? Just need to have a bit of advance time to line up

>Julian and David's schedules (and I'm out the week of August 12-16).

>Also: if you want to cut down on the time of the visit, ratcheting it

>down to something more like 60-90 minutes, or modify the agenda in any

>way, just let me know....

>

>Thoughts? Thanks!

>Todd

>

>-----Original Message-----

>From: Park, Todd

>Sent: Thursday, July 25, 2013 3:01 PM

>To: 'henry.chao' [mailto: [REDACTED]]

>Cc: 'Michelle.Snyder' [mailto: [REDACTED]]

>Subject: Re: Walk through of the online application in hc.gov

>

>Hi Henry, thanks so much! To provide more context, as I shared with

>Michelle, I'll be bringing David Simas and Julian Harris (Keith

>Fontenot's successor, newly arrived) with me. Would love to (1) walk

>through the current live online workflow (ideally from the start of the

>application through Plan Compare and selection) and (2) provide the

>opportunity for Julian to get the latest update on (a) IT dev, (b)

>testing, and (c) operational prep.

>
 >For (2), Julian is interested in one level of detail below the [REDACTED]
 >presentation. I would not prepare any custom materials whatsoever for
 >the meeting, but it would be great to show him (a) the slide you showed
 >me with all of the IT modules/completion dates, (b) the testing summary
 >for fed agencies, states, issuers you wrote up recently (I think for
 >someone's testimony), or similar material, and (c) a slide (if you have
 >it) of key operationalization steps (high level) on the road to Oct 1
 >and Dec 1 (e.g., contract X let, center X live, etc.).

>
 >Both Julian and David took great pains to ask that the visit not be
 >disruptive to your work -- I think that the message to give y'all the
 >space to rock and roll is spreading :)

>
 >So I'm thinking a focused two-hour visit, in Baltimore, going thru the
 >live workflow, and using high-level materials you already have.

>
 >Would next week be best, or would the week after be better, or would
 >either week be fine? I haven't yet pinged David and Julian for their
 >availability, but wanted to see what was optimal for you first. It
 >would be good to combine both of their visits, to save you time.
 >Thoughts on timing?

>
 >Michelle, it would be terrific for you to join -- would be great for
 >you to meet Julian and David, both of whom are terrific, and I've told
 >both of them that you and Henry are pure awesomeness :)

>
 >Thanks!
 >Todd

>
 >----- Original Message -----

>From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
 >Sent: Thursday, July 25, 2013 09:53 AM
 >To: Park, Todd
 >Cc: Oh, Mark U. (CMS/OIS) <[REDACTED]>; Coutts, Todd (CMS/OIS)
 ><[REDACTED]>; Outerbridge, Monique (CMS/OIS)
 ><[REDACTED]>; Grothe, Kirk A. (CMS/OIS)
 ><[REDACTED]>; Berkley, Katrina (CMS/OIS)
 ><[REDACTED]>; Rhones, Rhonda D. (CMS/OIS)
 ><[REDACTED]>; Graubard, Vivian
 ><[REDACTED]>; rich.martin <[REDACTED]>
 ><rich.martin@[REDACTED]>; cheryl.campbell <[REDACTED]>
 ><cheryl.campbell@[REDACTED]>; Lakshmi.Manambedu <[REDACTED]>
 ><Lakshmi.Manambedu@[REDACTED]>; Mark.Calem <[REDACTED]>
 ><Mark.Calem@[REDACTED]>; Paul.Weiss <[REDACTED]>; Wallace, Mary H.
 ><[REDACTED]>; Paul.Weiss <[REDACTED]>; Booth, Jon G. (CMS/OC)
 ><[REDACTED]>

>Subject: Walk through of the online application in hc.gov

>
 >Todd,
 >

>if you recall we had agreed to provide you a walk through and demo of
>the online application in its current form so you can get a chance to
>peek under the covers of hc.gov.
>
>Michelle mentioned you contacted her about this and that I should
>follow-up with you to schedule the walk through.
>
>Katrina can work with Vivian to find a window of opportunity next week
>if you agree.
>
>Let us know.
>
>Thanks.
>
>Henry Chao
>Deputy Chief Information Officer and Deputy Director Office of
>Information Services Centers for Medicare & Medicaid Services
>7500 Security Blvd
>Baltimore, MD 21244
>[REDACTED] (Pri)
>[REDACTED] (Alt)
>[REDACTED] (BB)

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Thursday, August 01, 2013 1:20 PM
To: Park, Todd; Snyder, Michelle (CMS/OA)
Cc: Graubard, Vivian; Mielke, Dawn M.; Outerbridge, Monique (CMS/OIS); Coutts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: Re: Walk through of the online application in hc.gov

Todd,

We have Lite Account Roll out through Monday and Issuer/trades coming in on Tuesday so earliest would be Wednesday or Thursday.

Henry Chao
 Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services

7500 Security Blvd
 Baltimore, MD 21244

[REDACTED] (Pri)
 [REDACTED] (Alt)
 [REDACTED] (BB)

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Thursday, August 01, 2013 01:10 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Cc: Graubard, Vivian <[REDACTED]>; Mielke, Dawn M. <[REDACTED]>; Outerbridge, Monique (CMS/OIS); Coutts, Todd (CMS/OIS)
Subject: RE: Walk through of the online application in hc.gov

Hi Henry/Michelle, just some additional scheduling intel to consider -- David Simas could be at CMS on Monday between 10 and 12:30. Julian will be there all morning, and says that he has meetings from 10 to 12. If Monday is a good day to do the visit -- and again, everyone is TOTALLY good with doing it another day, if that is better for you -- perhaps we try to do something in the 10 to 12 window on Marke tplace workflow walkthrough and general tech/ops updates, and Julian's other CMS meetings get moved earlier?

And again, totally good with picking another day entirely -- just let us know, thanks!

-----Original Message-----

From: Park, Todd
Sent: Wednesday, July 31, 2013 9:43 PM
To: 'henry.chao [REDACTED]'; 'Michelle.Snyder [REDACTED]';
Cc: Graubard, Vivian; Mielke, Dawn M.; 'monique.outerbridge [REDACTED]'; 'Todd.Coutts [REDACTED]';
Subject: Re: Walk through of the online application in hc.gov

Henry, absolutely no problem, and again, please don't hesitate to say that another day would work better -- we want to prioritize your operational imperatives above all other things!

----- Original Message -----

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]
Sent: Wednesday, July 31, 2013 08:13 PM
To: Park, Todd; Snyder, Michelle (CMS/OA) < [REDACTED]>
Cc: Graubard, Vivian; Mielke, Dawn M.; Outerbridge, Monique (CMS/OIS) < [REDACTED]>; Courts, Todd (CMS/OIS) < [REDACTED]>
Subject: Re: Walk through of the online application in hc.gov

I have asked the folks involved on the CMS and CGI slides if the 5th will work but it might take until tomorrow to confirm since it is the same people trying to get Lite Account launched.

Will respond as early as possible tomorrow morning.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

On 7/31/13 8:31 AM, "Park, Todd" < [REDACTED]> wrote:

>Hi Michelle, great -- Henry, please let me know if Aug 5 works for the
>mfg below; if so, I'll coordinate with Julian and David Simas to try to
>make sure that we can do 1 visit with all of us, for the sake of time
>efficiency for you and team.

>
>And Michelle, would love to chat! I can talk anytime between 9:30 and
>10:30, at 4:45, or at or any time after 6 pm. -- do any of those times
>work for you?

>
>Cheers,
>Todd

>
>----- Original Message -----

>>From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]
>>Sent: Wednesday, July 31, 2013 07:48 AM
>>To: Park, Todd; Chao, Henry (CMS/OIS) < [REDACTED]>
>>Subject: Re: Walk through of the online application in hc.gov

>>
>>I think Julian was looking to be here on the 5th. Haven't spoken with
>>Henry as to whether or not that works

>>
>>Also - Todd - is there a good time to call you today - I have a
>>propositiion for you that doesn't involve marketplaces for a change!!!!
>>

>live workflow, and using high-level materials you already have.
 >
 >Would next week be best, or would the week after be better, or would
 >either week be fine? I haven't yet pinged David and Julian for their
 >availability, but wanted to see what was optimal for you first. It
 >would be good to combine both of their visits, to save you time.
 >Thoughts on timing?
 >
 >Michelle, it would be terrific for you to join -- would be great for
 >you to meet Julian and David, both of whom are terrific; and I've told
 >both of them that you and Henry are pure awesomeness :)
 >
 >Thanks!
 >Todd
 >
 >

----- Original Message -----

>From: Chao, Henry (CMS/OIS) [mailto:]
 >Sent: Thursday, July 25, 2013 09:53 AM
 >To: Park, Todd
 >Cc: Oh, Mark U. (CMS/OIS) < >; Coats, Todd (CMS/OIS)
 >< >; Outerbridge, Monique (CMS/OIS)
 >< >; Grothe, Kirk A. (CMS/OIS)
 >< >; Berkley, Katrina (CMS/OIS)
 >< >; Rhones, Rhonda D. (CMS/OIS)
 >< >; Graubard, Vivian;
 >rich.martin <rich.martin >;
 >cheryl.campbell <cheryl.campbell >;
 >Lakshmi.Manambedu <Lakshmi.Manambedu >;
 >Mark.Calem <Mark.Calem >;
 >Paul.Weiss <Paul.Weiss >; Wallace, Mary H.
 >(CMS/OC) < >; Booth, Jon G. (CMS/OC)
 >< >
 >Subject: Walk through of the online application in hc.gov

>
 >Todd,
 >
 >if you recall we had agreed to provide you a walk through and demo of
 >the online application in its current form so you can get a chance to
 >peek under the covers of hc.gov.
 >
 >Michelle mentioned you contacted her about this and that I should
 >follow-up with you to schedule the walk through.
 >
 >Katrina can work with Vivian to find a window of opportunity next week
 >if you agree.
 >
 >Let us know.
 >
 >Thanks.
 >
 >Henry Chao

From: Park, Todd
Sent: Thursday, August 01, 2013 1:20 PM
To: 'henry.chao'; 'Michelle.Snyder'
Cc: Graubard, Vivian; Mielke, Dawn M.; 'monique.outerbridge'; 'Todd.Couts'
Subject: RE: Walk through of the online application in hc.gov

Apologies, additional schedule intel. It turns out that David Simas can be out of the office from 10 to 12:30, INCLUDING travel time. So: what could work, perhaps, is an 11 to 12:30 meeting in Baltimore, where the first 45 minutes is a walkthrough of the live user workflow (with David, Julian, and me) and the second 45 minutes is the general tech/ops update (with just Julian and me). And again, if this doesn't work for you, totally cool, we'll schedule it for some other day. Just let us know, thanks!

-----Original Message-----

From: Park, Todd
Sent: Thursday, August 01, 2013 1:11 PM
To: 'henry.chao'; 'Michelle.Snyder'
Cc: Graubard, Vivian; Mielke, Dawn M.; 'monique.outerbridge'; 'Todd.Couts'
Subject: RE: Walk through of the online application in hc.gov

Hi Henry/Michelle, just some additional scheduling intel to consider -- David Simas could be at CMS on Monday between 10 and 12:30. Julian will be there all morning, and says that he has meetings from 10 to 12. If Monday is a good day to do the visit -- and again, everyone is TOTALLY good with doing it another day, if that is better for YOU -- perhaps we try to do something in the 10 to 12 window on Marketplace workflow walkthrough and general tech/ops updates, and Julian's other CMS meetings get moved earlier?

And again, totally good with picking another day entirely -- just let us know, thanks!

-----Original Message-----

From: Park, Todd
Sent: Wednesday, July 31, 2013 9:43 PM
To: 'henry.chao'; 'Michelle.Snyder'
Cc: Graubard, Vivian; Mielke, Dawn M.; 'monique.outerbridge'; 'Todd.Couts'
Subject: Re: Walk through of the online application in hc.gov

Henry, absolutely no problem, and again, please don't hesitate to say that another day would work better -- we want to prioritize your operational imperatives above all other things!

-----Original Message-----

From: Chao, Henry (CMS/OIS) [mailto:];
Sent: Wednesday, July 31, 2013 08:13 PM
To: Park, Todd; Snyder, Michelle (CMS/OA) < >
Cc: Graubard, Vivian; Mielke, Dawn M.; Outerbridge, Monique (CMS/OIS) < >; Couts, Todd (CMS/OIS) < >
Subject: Re: Walk through of the online application in hc.gov

>Deputy Chief Information Officer and Deputy Director Office of
>Information Services Centers for Medicare & Medicaid Services
>7500 Security Blvd
>Baltimore, MD 21244

Y [REDACTED] (Pri)
Y [REDACTED] (Alt)
Y [REDACTED] (BB)

From: Park, Todd
Sent: Thursday, August 01, 2013 3:03 PM
To: Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; michelle.snyder [REDACTED]; henry.chao [REDACTED]; Outerbridge, Monique (CMS/OIS); Couts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: RE: CMS visit update -- Wed or Fri next week possible?

Sorry, re-sending with corrected email subject line ☺

From: Park, Todd
Sent: Thursday, August 01, 2013 3:03 PM
To: Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; michelle.snyder [REDACTED]; henry.chao [REDACTED]; Outerbridge, Monique (CMS/OIS); Couts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: CMS visit update -- Wed or Thurs next week possible?

Hi Julian and David, with respect to the CMS Marketplace live workflow walkthrough/tech ops update meeting: it looks like the earliest the CMS tech team can do the meeting is Wed (8/7), Thurs (8/8), or Friday (8/9) next week. (Mon/Tues will be consumed by Lite Account rollout and issuer meetings).

~~I could conceivably do a CMS visit the morning of Wed, 8/7, anytime between 8 and 11:30 (I'd have to leave Baltimore by 11:30), or the morning of Friday, 8/9, anytime between 8 and 12 pm.~~

Julian/David, would either/both of those slots work for you?

I think we're looking for a 90 minute block of time to be in Baltimore (the workflow walkthrough/discussion would be 45 minutes of that time).

Looping Team CMS and Dawn/Viv...

Dawn/Viv will help coordinate.... Hopefully we can find a time next week that works for all.... Thanks!

Todd

From: Park, Todd
Sent: Thursday, August 01, 2013 3:03 PM
To: Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; michelle.snyder [REDACTED];
henry.chao [REDACTED]; O'Leary, Monique (CMS/OIS); Couts, Todd (CMS/OIS);
Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: CMS visit update -- Wed or Thurs next week possible?

Hi Julian and David, with respect to the CMS Marketplace live workflow walkthrough/tech ops update meeting: it looks like the earliest the CMS tech team can do the meeting is Wed (8/7), Thurs (8/8), or Friday (8/9) next week. (Mon/Tues will be consumed by Lite Account rollout and issuer meetings).

I could conceivably do a CMS visit the morning of Wed, 8/7, anytime between 8 and 11:30 (I'd have to leave Baltimore by 11:30), or the morning of Friday, 8/9, anytime between 8 and 12 pm.

Julian/David, would either/both of those slots work for you?

I think we're looking for a 90 minute block of time to be in Baltimore (the workflow walkthrough/discussion would be 45 minutes of that time).

Looping Team CMS and Dawn/Viv....

Dawn/Viv will help coordinate.... Hopefully we can find a time next week that works for all.... Thanks!

Todd

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Thursday, August 01, 2013 4:28 PM
To: Park, Todd; Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; Snyder, Michelle (CMS/OA); Outerbridge, Monique (CMS/OIS); Couts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Best time for my staff and CGI is Friday 8/9.

Henry Chao
 Deputy CIO & Deputy Director,
 Office of Information Services
 Centers for Medicare & Medicaid Services

From: Todd Park <[REDACTED]>
Date: Thu, 1 Aug 2013 19:03:24 +0000
To: "Harris, Julian" <[REDACTED]>, "Simas, David M." <[REDACTED]>
Cc: "Mielke, Dawn M." <[REDACTED]>, "Graubard, Vivian" <[REDACTED]>, Michelle Snyder <[REDACTED]>, HENRY CHAO <[REDACTED]>, Monique Outerbridge <[REDACTED]>, Todd Couts <[REDACTED]>, Mary Wallace <[REDACTED]>, Jon Booth <[REDACTED]>
Subject: RE: CMS visit update -- Wed or Fri next week possible?

Sorry, resending with corrected email subject line ☺

From: Park, Todd
Sent: Thursday, August 01, 2013 3:03 PM
To: Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; michelle.snyder <[REDACTED]>; henry.chao <[REDACTED]>; Outerbridge, Monique (CMS/OIS); Couts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: CMS visit update -- Wed or Thurs next week possible?

Hi Julian and David, with respect to the CMS Marketplace live workflow walkthrough/tech ops update meeting: It looks like the earliest the CMS tech team can do the meeting is Wed (8/7), Thurs (8/8), or Friday (8/9) next week. (Mon/Tues will be consumed by Lite Account rollout and issuer meetings).

I could conceivably do a CMS visit the morning of Wed, 8/7, anytime between 8 and 11:30 (I'd have to leave Baltimore by 11:30); or the morning of Friday, 8/9, anytime between 8 and 12 pm.

Julian/David, would either/both of those slots work for you?

I think we're looking for a 90 minute block of time to be in Baltimore (the workflow walkthrough/discussion would be 45 minutes of that time).

Looping Team CMS and Dawn/Viv...

Dawn/Viv will help coordinate.... Hopefully we can find a time next week that works for all... Thanks!

Todd

From: Todd Park <[REDACTED]>
 Date: Thu, 1 Aug 2013 19:03:24 +0000
 To: "Harris, Julian" <[REDACTED]>, "Simas, David M." <[REDACTED]>
 Cc: "Mielke, Dawn M." <[REDACTED]>, "Graubard, Vivian" <[REDACTED]>
 Michelle Snyder <[REDACTED]>, HENRY CHAO <[REDACTED]>, Monique Outerbridge
 <[REDACTED]>, Todd Coutts <[REDACTED]>, Mary Wallace
 <[REDACTED]>, Jon Booth <[REDACTED]>
 Subject: RE: CMS visit update -- Wed or Fri next week possible?

Sorry, resending with corrected email subject line @

From: Park, Todd
 Sent: Thursday, August 01, 2013 3:03 PM
 To: Harris, Julian; Simas, David M.
 Cc: Mielke, Dawn M.; Graubard, Vivian; michelle.snyder <[REDACTED]>; henry.chao <[REDACTED]>; Outerbridge, Monique
 (CMS/OIS); Coutts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
 Subject: CMS visit update -- Wed or Thurs next week possible?

Hi Julian and David, with respect to the CMS Marketplace live workflow walkthrough/tech ops update meeting: it looks like the earliest the CMS tech team can do the meeting is Wed (8/7), Thurs (8/8), or Friday (8/9) next week. (Mon/Tues will be consumed by Lite Account rollout and issuer meetings).

I could conceivably do a CMS visit the morning of Wed, 8/7, anytime between 8 and 11:30 (I'd have to leave Baltimore by 11:30), or the morning of Friday, 8/9, anytime between 8 and 12 pm.

Julian/David, would either/both of those slots work for you?

I think we're looking for a 90 minute block of time to be in Baltimore (the workflow walkthrough/discussion would be 45 minutes of that time).

Looping Team CMS and Dawn/Viv...

Dawn/Viv will help coordinate.... Hopefully we can find a time next week that works for all.... Thanks!

Todd

To: 'Todd Y Park' <[redacted]> <Todd Y Park [redacted]>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Can you give me a call real quick?
[redacted]

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[redacted] (Pri)
[redacted] (Alt)
[redacted] (BB)

From: Park, Todd [mailto:[redacted]]
Sent: Thursday, August 01, 2013 06:56 PM
To: Harris, Julian <[redacted]>; Chao, Henry (CMS/OIS); Simas, David M.
<[redacted]>;
Cc: Mielke, Dawn M. <[redacted]>; Graubard, Vivian <[redacted]>; Snyder, Michelle (CMS/OA); Outerbridge, Monique (CMS/OIS); Coutts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: RE: CMS visit update -- Wed or Fri next week possible?

How about Thursday, 8/8, starting at 5 pm (or later)? (Henry, we should be back from Culpeper by then, yes?)

From: Harris, Julian
Sent: Thursday, August 01, 2013 4:49 PM
To: 'henry.chao [redacted]'; Park, Todd; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; Michelle.Snyder [redacted]; monique.outerbridge [redacted]; Todd.Coutts [redacted]; Mary.Wallace [redacted]; Jon.Booth [redacted]
Subject: Re: CMS visit update -- Wed or Fri next week possible?

I'm unavailable on Friday..

From: Chao, Henry (CMS/OIS) [mailto:[redacted]]
Sent: Thursday, August 01, 2013 04:27 PM
To: Park, Todd; Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; Snyder, Michelle (CMS/OA) <[redacted]>; Outerbridge, Monique (CMS/OIS) <[redacted]>; Coutts, Todd (CMS/OIS) <[redacted]>; Wallace, Mary H. (CMS/OC) <[redacted]>; Booth, Jon G. (CMS/OC) <[redacted]>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Best time for my staff and CGI is Friday 8/9.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

demonstrating the Online Streamlined Application (in "beta") for her and a select group the week of 8/26.

We can include in our trip to visit with Verizon-Terremark in Culpeper next Thursday 8/8 a visit to CGI in Herndon and give you a demo, but it would only be you.

Your choices are then get a demo by yourself next Thursday or come as part of Marilyn's walk through the week of 8/26.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

(Pri)
(Alt)
(BB)

From: Chao, Henry (CMS/OIS)
Sent: Friday, August 02, 2013 10:13 AM
To: 'Todd Y Park' <Todd.Y.Park@cms.gov>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Can you give me a call real quick?

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

(Pri)
(Alt)
(BB)

From: Park, Todd [mailto:]
Sent: Thursday, August 01, 2013 06:56 PM
To: Harris, Julian < >; Chao, Henry (CMS/OIS); Simas, David M. < >
Cc: Mielke, Dawn M. < >; Graubard, Vivian < >; Snyder, Michelle (CMS/OA); Outerbridge, Monique (CMS/OIS); Couts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jpn G. (CMS/OC)
Subject: RE: CMS visit update -- Wed or Fri next week possible?

How about Thursday, 8/8, starting at 5 pm (or later)? (Henry, we should be back from Culpeper by then, yes?)

From: Harris, Julian
Sent: Thursday, August 01, 2013 4:49 PM
To: 'henry.chao' < >; Park, Todd; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; 'Michelle.Snyder' < >; 'monique.outerbridge' < >

From: Park, Todd
Sent: Tuesday, August 06, 2013 3:43 PM
To: Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Coutts, Todd (CMS/OIS); Outerbridge, Monique (CMS/OIS); Kerr, James T. (CMS/CMHPO); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Reilly, Megan C. (CMS/OC); Mielke, Dawn M.; Graubard, Vivian
Subject: RE: CMS visit update -- Wed or Fri next week possible?

OK, great, thank you! Michelle, should I call you at your office?

From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]
Sent: Tuesday, August 06, 2013 3:06 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Coutts, Todd (CMS/OIS); Outerbridge, Monique (CMS/OIS); Kerr, James T. (CMS/CMHPO); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Reilly, Megan C. (CMS/OC); Mielke, Dawn M.; Graubard, Vivian
Subject: Re: CMS visit update -- Wed or Fri next week possible?

430

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto: [REDACTED]]
Sent: Tuesday, August 06, 2013 12:40 PM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Coutts, Todd (CMS/OIS); Outerbridge, Monique (CMS/OIS); Kerr, James T. (CMS/CMHPO); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Reilly, Megan C. (CMS/OC); Mielke, Dawn M. < [REDACTED] >; Graubard, Vivian < [REDACTED] >
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Henry, sounds good -- can we jump on the phone for 5 min today just to finalize what we should do on this front and with David/Julian? Michelle, would be great if you could join as well.... Would a time between 3:30 and 5 work, or at anytime after 6 today? Will just be 5 minutes.... Thanks!

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]
Sent: Friday, August 02, 2013 10:41 AM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA) < [REDACTED] >; Coutts, Todd (CMS/OIS) < [REDACTED] >; Outerbridge, Monique (CMS/OIS) < [REDACTED] >; Kerr, James T. (CMS/CMHPO) < [REDACTED] >; Wallace, Mary H. (CMS/OC) < [REDACTED] >; Booth, Jon G. (CMS/OC) < [REDACTED] >; Reilly, Megan C. (CMS/OC) < [REDACTED] >
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Todd,

I just spoke to Michelle and this is the direction we will go based on her "guidance."

Marilyn wants a walk through of what has been built, basically the same thing you are asking for except we are

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Tuesday, August 06, 2013 3:06 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Coutts, Todd (CMS/OIS); Outerbridge, Monique (CMS/OIS); Kerr, James T. (CMS/CMHPO); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Reilly, Megan C. (CMS/OC); Mielke, Dawn M.; Graubard, Vivian
Subject: Re: CMS visit update -- Wed or Fri next week possible?

430

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, August 06, 2013 12:40 PM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Coutts, Todd (CMS/OIS); Outerbridge, Monique (CMS/OIS); Kerr, James T. (CMS/CMHPO); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC); Reilly, Megan C. (CMS/OC); Mielke, Dawn M. <[REDACTED]>; Graubard, Vivian <[REDACTED]>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Henry, sounds good -- can we jump on the phone for 5 min today just to finalize what we should do on this front and with David/Julian? Michelle, would be great if you could join as well.... Would a time between 3:30 and 5 work, or at anytime after 6 today? Will just be 5 minutes.... Thanks!

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Friday, August 02, 2013 10:41 AM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA) <[REDACTED]>; Coutts, Todd (CMS/OIS) <[REDACTED]>; Outerbridge, Monique (CMS/OIS) <[REDACTED]>; Kerr, James T. (CMS/CMHPO) <[REDACTED]>; Wallace, Mary H. (CMS/OC) <[REDACTED]>; Booth, Jon G. (CMS/OC) <[REDACTED]>; Reilly, Megan C. (CMS/OC) <[REDACTED]>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Todd,

I just spoke to Michelle and this is the direction we will go based on her "guidance."

Marilyn wants a walk through of what has been built, basically the same thing you are asking for except we are demonstrating the Online Streamlined Application (in "beta") for her and a select group the week of 8/26.

We can include in our trip to visit with Verizon -Terremark in Culpeper next Thursday 8/8 a visit to CGI in Herndon and give you a demo, but it would only be you.

Your choices are then get a demo by yourself next Thursday or come as part of Marilyn's walk through the week of 8/26.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[Redacted] (Pri)
[Redacted] (Alt)
[Redacted] (BB)

From: Chao, Henry (CMS/OIS)
Sent: Friday, August 02, 2013 10:13 AM
To: 'Todd Y Park' <[Redacted]>; <Todd Y Park [Redacted]>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Can you give me a call real quick?

[Redacted]

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

[Redacted] (Pri)
[Redacted] (Alt)
[Redacted] (BB)

From: Park, Todd [mailto:[Redacted]]
Sent: Thursday, August 01, 2013 06:56 PM
To: Harris, Julian <[Redacted]>; Chao, Henry (CMS/OIS); Simas, David M. <[Redacted]>; Mielke, Dawn M. <[Redacted]>; Graubard, Vivian <[Redacted]>; Snyder, Michelle (CMS/OA); Outerbridge, Monique (CMS/OIS); Coutts, Todd (CMS/OIS); Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: RE: CMS visit update -- Wed or Fri next week possible?

How about Thursday, 8/8, starting at 5 pm (or later)? (Henry, we should be back from Culpeper by then, yes?)

From: Harris, Julian
Sent: Thursday, August 01, 2013 4:49 PM
To: 'henry.chao' <[Redacted]>; Park, Todd; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; Michelle.Snyder <[Redacted]>; monique.outerbridge <[Redacted]>; Todd.Coutts <[Redacted]>; Mary.Wallace <[Redacted]>; Jon.Booth <[Redacted]>
Subject: Re: CMS visit update -- Wed or Fri next week possible?

I'm unavailable on Friday.

From: Chao, Henry (CMS/OIS) [mailto:[Redacted]]
Sent: Thursday, August 01, 2013 04:27 PM
To: Park, Todd; Harris, Julian; Simas, David M.
Cc: Mielke, Dawn M.; Graubard, Vivian; Snyder, Michelle (CMS/OA) <[Redacted]>; Outerbridge,

From: Tavanner, Marilyn (CMS/OA) <[REDACTED]>
Sent: Thursday, August 22, 2013 10:20 AM
To: Park, Todd; Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Khalid, Aryana C. (CMS/OA); Cavanaugh, Alicia A. (CMS/OA); Miller, Ruth A. (CMS/OA)
Subject: Re: CMS visit update -- Wed or Fri next week possible?

I am on vacation next week. We can do the walk through the week of Sept 3rd. Aryana and I will join. Alicia and Sam can coordinate.

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, August 20, 2013 07:07 PM
To: Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Tavanner, Marilyn (CMS/OA)
Subject: RE: CMS visit update -- Wed or Fri next week possible?

Hi Michelle and Henry, one additional note (and looping Marilyn on this as well) if possible, Tara McGuinness would like to join Julian, David Simas, and me on the walkthrough with Marilyn, and Chris Jennings likely will as well.

It should all happen at the same time Marilyn does her walkthrough, so as to economize use of CMS time.

And a date constraint: David Simas will be out starting tomorrow through August 27, so, if possible, it would be great for the walkthrough to happen Aug 28 or later.

When you think you know a date or possible dates, please let me know, and we'll get folks lined up here to go to Baltimore.

Thanks very much!
 Todd

From: Park, Todd
Sent: Tuesday, August 20, 2013 9:14 AM
To: 'Michelle.Snyder [REDACTED]'; 'henry.chao [REDACTED]'
Subject: RE: CMS visit update -- Wed or Fri next week possible?

Hi Michelle and Henry, one additional thought: was wondering if I might be able to drop by some evening this week for a few minutes to say hi to the tech team (whomever might be around at that particular moment), bring them cookies (literally), and just say thank you for the massive effort they are putting in during this home stretch. I can only imagine how crazy/intense it must be right now and just wanted to come by for a few minutes to say thank you. And since I'll only be risking my own life, I'll be delighted to drive myself to and from Baltimore to do so @. Would it be OK to drop by this week?

From: Park, Todd
Sent: Monday, August 19, 2013 7:38 PM
To: 'Michelle.Snyder [REDACTED]'; 'henry.chao [REDACTED]'
Subject: Re: CMS visit update -- Wed or Fri next week possible?

Hi Michelle and Henry,

Michelle, hope Santa Fe was terrific!

Two quick questions:

1. With respect to the walkthrough with Marilyn (which David, Julian, and I would join), any update on when this will happen? Just want to get calendars aligned...
2. Henry, might you have 5 min in the next few days to chat about a cybersecurity question? I can chat in the evening any time if that is more convenient for you...

Thanks so much,
Todd

From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]
Sent: Wednesday, August 07, 2013 09:20 AM
To: Park, Todd; Rzczkowski, Kristin; Mielke, Dawn M.; Harris, Julian; Chao, Henry (CMS/OIS)
 < [REDACTED] >; Simas, David M.; Armstead, Andrea E. (CMS/OA) < [REDACTED] >
Cc: Graubard, Vivian; Outerbridge, Monique (CMS/OIS) < [REDACTED] >; Coutts, Todd (CMS/OIS)
 < [REDACTED] >; Wallace, Mary H. (CMS/OC) < [REDACTED] >; Booth, Jon G. (CMS/OC)
 < [REDACTED] >
Subject: RE: CMS visit update -- Wed or Fri next week possible?

Works well for CMS

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto: [REDACTED]]
Sent: Tuesday, August 06, 2013 08:11 PM
To: Rzczkowski, Kristin < [REDACTED] >; Snyder, Michelle (CMS/OA); Mielke, Dawn M.
 < [REDACTED] >; Harris, Julian < [REDACTED] >; Chao, Henry (CMS/OIS); Simas,
 David M. < [REDACTED] >; Armstead, Andrea E. (CMS/OA)
Cc: Graubard, Vivian < [REDACTED] >; Outerbridge, Monique (CMS/OIS); Coutts, Todd. (CMS/OIS);
 Wallace, Mary H. (CMS/OC); Booth, Jon G. (CMS/OC)
Subject: RE: CMS visit update -- Wed or Fri next week possible?

Hi team, here's a proposed gameplan, which should hopefully ease the degree of scheduling difficulty involved here and also ensure we make judicious use of CMS bandwidth:

1. Team CMS is planning to walk Marilyn through the consumer experience and workflow at some point in the Aug 26-28 date range. I propose that David, Julian, and I join Marilyn for that walkthrough. CMS may host this walkthrough in the Columbia command center, in which case we'd get to check this out as well! Though we have to promise not to touch anything in the command center ☺
2. Separately, Julian would visit CMS in Baltimore to get up to speed on a range of topics he would like to get up to speed on, including the latest with respect to Marketplace ops/IT. It looks like the week of August 19 would be a great week for this (Michelle Snyder is out next week). I suggest that Kristin and Andi work to put together an agenda that would be best for Julian, based on what Julian already knows he wants to cover and additional topics CMS would suggest Julian cover as well. This visit can be Julian solo, without David and me. I would very much like to go if I can, for the Marketplace section of the day in particular but don't let me be a scheduling bottleneck.

From: Simas, David M.
Sent: Wednesday, September 11, 2013 7:50 AM
To: 'Marilyn.Tavener [mailto: [REDACTED]]';
Cc: 'Aryana.Khalid [mailto: [REDACTED]]'; Park, Todd; Lambrew, Jeanne;
'Alicia.Cavanaugh [mailto: [REDACTED]]';
Subject: Re: demo this morning

Makes sense.

Thanks Marilyn.

From: Tavener, Marilyn (CMS/OA) [mailto: [REDACTED]]
Sent: Wednesday, September 11, 2013 07:46 AM
To: Simas, David M.
Cc: Khalid, Aryana C. (CMS/OA) < [REDACTED] >; Park, Todd; Lambrew, Jeanne; Cavanaugh, Alicia A. (CMS/OA) < [REDACTED] >
Subject: demo this morning

David-wanted to make you aware that for your demo -we will be working from a demo platform and not "live" on the system....we did "live" on the system last week for the larger group -but did not want to take the system down today for demo purposes for you or the Secretary as we have an entire team working in Herndon including alpha testers....it will look and feel the same but wanted you to know....just sent the Secretary the same message...thanks and look forward to seeing you shortly...Marilyn

From: Tavener, Marilyn (CMS/OA) <[REDACTED]>
Sent: Wednesday, September 11, 2013 7:47 AM
To: Sīmas, David M.
Cc: Khalid, Aryana C. (CMS/OA); Park, Todd; Lambrew, Jeanne; Cavanaugh, Alicia A. (CMS/OA)
Subject: demo this morning

David-wanted to make you aware that for your demo -we will be working from a demo platform and not "live" on the system....we did "live" on the system last week for the larger group -but did not want to take the system down today for demo purposes for you or the Secretary as we have an entire team working in Herndon including alpha testers...it will look and feel the same but wanted you to know..... just sent the Secretary the same message...thanks and look forward to seeing you shortly....Marilyn

From: Tavenner, Marilyn (CMS/OA) <[REDACTED]>
Sent: Tuesday, September 24, 2013 3:27 PM
To: Park, Todd; Snyder, Michelle (CMS/OA)
Cc: Chao, Henry (CMS/OIS)
Subject: RE: Herndon Information/Instructions.

Yes I am very frightened!!

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, September 24, 2013 3:23 PM
To: Snyder, Michelle (CMS/OA); Tavenner, Marilyn (CMS/OA)
Cc: Chao, Henry (CMS/OIS)
Subject: Re: Herndon Information/Instructions

Will absolutely obey all instructions with precision!! And really looking forward to the visit -- and more than anything, thanking everyone from the bottom of our collective hearts for the truly incredible work they are doing :)

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]
Sent: Tuesday, September 24, 2013 02:42 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA) <[REDACTED]>
Cc: Chao, Henry (CMS/OIS) <[REDACTED]>
Subject: Herndon Information/Instructions

I have requested that the security cameras at Herndon be loaded with facial recognition software so that if either of you wander into a restricted area armed with a set of questions alarms will sound. Henry has been issued a government taser if the visit extends beyond an hour or if Todd looks for a later ride home.....that ought to scare both of you.....Henry, armed and dangerous ☺

Enjoy the visit.

Michelle

A.Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

From: Tavenner, Marilyn (CMS/OA) <[REDACTED]>
Sent: Tuesday, September 24, 2013 6:36 PM
To: Snyder, Michelle (CMS/OA); Park, Todd
Cc: Chao, Henry (CMS/OIS)
Subject: Re: Herndon Information/Instructions

I kept Todd under control (well sort of). Henry thanks for a great visit!!!

From: Snyder, Michelle (CMS/OA)
Sent: Tuesday, September 24, 2013 02:42 PM
To: Park, Todd ([REDACTED]) <[REDACTED]>; Tavenner, Marilyn (CMS/OA)
Cc: Chao, Henry (CMS/OIS)
Subject: Herndon Information/Instructions

I have requested that the security cameras at Herndon be loaded with facial recognition software so that if either of you wander into a restricted area armed with a set of questions alarms will sound. Henry has been issued a government taser if the visit extends beyond an hour or if Todd looks for a later ride home.....that ought to scare both of you.....Henry, armed and dangerous ☺

Enjoy the visit.

Michelle

A. Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Tuesday, June 11, 2013 8:29 PM
To: Park, Todd
Cc: Graubard, Vivian; Snyder, Michelle (CMS/OA)
Subject: Re: Sync-up

Hi Todd,

I am out next week so probably the week after will work for me.

As for issue around logos, I'm not sure you have the complete scoop but I suppose this issue got to you because people can't accept that we can't do this as easily as one might think and the fallout from catering to the Blues (as opposed to the AHIP members) will triple the confusion and cause more grief than we can handle. In addition because I have looked at this carefully along with Mary Wallace, Jon Booth, Jim Kerr, Michelle, and our developers (and including the BCBSA IT leads that think it's as easy as changing colors on a website), if you twist my arm and make me do magic to render logos correctly for 100% of the OHPs in millions of plan compare results where I have to map/link to a data source outside of HIOS, well, it would just make a liar out of me for saying no when someone can make me say yes.

If you want to talk about this then call me any time. If we're going to talk logos at this one hour catch -up session it will then not be a great use of our time and may get me in to more trouble because no one will believe me anymore because I hold the line on something that in the grand scheme no one would really want us to trade off for more risk.

Thanks for understanding.

Henry Chao
 Deputy Chief Information Officer and Deputy Director
 Office of Information Services
 Centers for Medicare & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244
 [REDACTED] (Pri)
 [REDACTED] (Alt)
 [REDACTED] (BB)

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, June 11, 2013 07:52 PM
To: Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Tavenner, Marilyn (CMS/OA); VanRoekel, Steven <[REDACTED]>; Graubard, Vivian <[REDACTED]>; Lynch, Laura <[REDACTED]>
Subject: Sync-up

Hi Michelle and Henry, hope all is terrific with you!

As you've heard from Marilyn, would love (with Steve) to arrange time (1 hour) in the next week or week and half to check in on how things are going with respect to Marketplace IT dev and testing. (And also to discuss the tactical question of issuer logos). Would love to arrange a visit to Baltimore, but given how crazy schedules are, I'm guessing that a videoconference or conference call would be more feasible.

We don't need any special documentation or whatnot. Just you ☺ If you have something that you've already put together for another purpose that you'd like to send, great.

May Vivian and Laura work with your office to set up a time to chat?

Cheers,
Todd

From: Graubard, Vivian
Sent: Friday, June 28, 2013 8:54 AM
To: Chao, Henry (CMS/OIS); Park, Todd
Subject: RE: Follow-up

Let's go with July 16th from 4-8. Does that still work? Does anyone else from WH need to join?

Thanks,
Viv

From: Chao, Henry (CMS/OIS) [mailto:██████████]
Sent: Wednesday, June 26, 2013 11:16 PM
To: Park, Todd
Cc: Graubard, Vivian
Subject: Re: Follow-up

Todd,

For planning purposes I am blocking the following dates and times. Let me know which works for you. Thanks!

Monday July 8 5pm to at least 9pm
Tuesday July 9 4pm to at least 8pm
Monday July 15 5pm to at least 9pm
Tuesday July 16 4pm to at least 8pm

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

██████████ (Pri)
██████████ (Alt)
██████████ (BB)

From: Park, Todd [mailto:██████████] *Logos*
Sent: Wednesday, June 26, 2013 05:34 PM
To: Tavenner, Marilyn (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Follow-up

Hi Marilyn, Michelle, and Henry,

After talking with Henry and team, I spoke with Mark about the logo issue, and explained why attempting to add logos for October 1 is extremely unwise. He understands. He may want me to get on the phone with someone from the Blu as so they fully understand it. I'm more than happy to do so on your behalf this issue should not consume any more of your time.

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Wednesday, June 26, 2013 1:52 PM
To: Park, Todd; Snyder, Michelle (CMS/OA)
Cc: Kerr, James T. (CMS/CMHPO); Wallace, Mary H. (CMS/OC); Outerbridge, Monique (CMS/OIS); Bowen, Marianne (CMS/OA)
Subject: Re: Draft writeup

Here's the write-up. I'm sending and copying those who are key to supporting this assertion.

Attempting to integrate logos into the FFM for October 1, 2014 is not possible with less than 100 days left. This is not because the "concept" of integrating a logo is by itself a difficult thing to do. In reality and practice it's not possible at this point because of inter-dependencies with other processes, the already underway testing processes with dedicated test data, schedule/lack of time, and resource constraints. Specifics are:

The operational execution process of acquiring logos requires coordination with NAIC and their SERFF system since Issuers in approximately 11 or so FFM states submit their data through the SERFF system and not directly to HIOS (this was a policy decision made late last summer). Any change in how Issuers submit data and how it ends up as part of the FFM operations requires coordination not just with Issuers but also with NAIC and their SERFF development and operations team.

The logo by itself may be considered as a simple image object, but in reality is still a piece of data that needs to be managed in a structured and controlled manner in order to display it properly each and every time. If the Logo/data was not factored in the design of how data are submitted as part of the QHP process, that means it has to be done in a "one-off" manner outside of the established automated processes for Plan Compare. Outside of the automated process will mean the ability to attach the correct logo to the right row or column of Plan Compare results (rendered literally millions of times from consumers constantly requesting compare results for their input to appreciate the volume of transactions just think in terms of consumers seeing responses to their search when they provide input to Priceline, Expedia, Travelocity, etc. except in this case it's multiplied by the number of consumers coming in to the FFM and their requests to compare plans).

At this time amidst the final stages of working with Issuers, DOIs, and NAIC to finalize a validated set of QHP data nationally by July 31, 2013, altering HIOS, getting NAIC to alter SERFF, and working with Issuers that may or may not voluntarily submit logos is not feasible and endangers the ability to stay on schedule. Collecting any additional data from Issuers via templates or some other process, loading these data either directly into the HIOS system or outside the HIOS system in a manually established data store and process, validating the data, have NAIC/SERFF send the new logo data separately from QHP data to CMS, and having the rating engine retrieve and render that data when the FFM design and build process has been locked down and we are in the middle of crunch-time between now to October 1, would introduce significant risk to getting the FFM fundamental capabilities in place for open enrollment. Think of it as trying to change a gear in an airplane engine in mid-flight. Or adding a new field to an IRS tax form in the middle of filing season. As an isolated act without the constraints of schedule and scope, adding the data isn't impossible. What's impossible is the notion of adding it to the tax form via a system modification when that system is going through an intense time, with a lot of moving parts involved, and where a wrong move could actually screw the whole system up and in the case of attempting to add a logo and screwing that up means we will adversely impact enrollment and the consumer experience.

There exists the notion that as an alternative to changing the core plan data submission/management process and systems (i.e., modifying the carrier plan data templates, HIOS, the QHP database, and rating engine logic) would be to set up a separate database of logos outside this core data and process already in place with QHP

submission in conjunction with NAIC and have the FFM system, when rendering a given Issuer's QHP product, pull separately from both the QHP database plus the logo database and then "join" the results and display to the consumer. This is a terrible idea technically, would be extremely prone to error, and still creates the issue of mucking with the jet engine while it's in flight.

The current commitment to the scope and delivery schedule to make October 1, 2013 is locked down in terms of committed hours from our contractors. Anything that was not part of scope means we have to negotiate across the board with CCIO, CMCS, OC, and our contractors to find hours to take away and recommit to this effort there are no available hours at this point to freely use as commitment arise that were not planned months in advance and funded as part of a contract.

The right way to add logos to the FFM would be to modify the core plan data submission/management process and systems to include logos as part of the issuer QHP product templates and be able to process logos in an automated, structured, and high precision all the way through. This is not possible for Oct 1, 2013 without introducing significant operational risk to the go-live, as discussed above. We suggest considering it as part of a future release, post October 1 understanding that it will have to compete with a lot of priorities. The reasonable thing to do would be to target making this modification in time for the next cycle of plan bids in 2014 starting with the Payment Notice for 2015 that will be released in the March 2014 timeframe and logos can start flowing in as part of QHP submission in the June -July 2014 timeframe.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services

From: Todd Park <[REDACTED]>
Date: Wed, 26 Jun 2013 02:03:17 +0000
To: Michelle Snyder <[REDACTED]>, HENRY CHAO <[REDACTED]>
Subject: RE: Draft writeup

Attempting to integrate logos into the FFM for October 1 is not advisable. This is not because the act of integrating a logo is by itself a difficult thing to do. It's because the process for collecting health plan and product data from carriers via templates, loading these data into the HIOS system, validating the data, transferring the data from HIOS into the FFM QHP database, and having the rating engine retrieve and render that data in the FFM has been locked down, and is being utilized to support plan data collection/validation and system testing as we speak. Changing the underlying plan data template and processing routine right now -- by adding a new plan data element, the logo -- during the crunch-time sprint we're in from now to October 1, would introduce significant risk. Think of it as trying to change a gear in an airplane engine in mid-flight. Or adding a new field to an IRS tax form in the middle of filing season. As an isolated act, adding the field isn't hard. What's hard is the notion of adding it to the tax form via a system modification when that system is going through an intense time, with a lot of moving parts involved, and where a wrong move could actually screw the whole system up.

An alternative to changing the core plan data submission/management process and systems (i.e., modifying the carrier plan data templates, HIOS, the QHP database, and rating engine logic) would be to set up a database of logos outside this core data management process and have the FFM system, when rendering a given insurance product, pull from both the QHP database plus the logo database. This is a terrible idea technically, would be prone to error, and still creates the issue of mucking with the jet engine while it's in flight.

303

From: Tavener, Marilyn (CMS/OA) <[REDACTED]>
Sent: Wednesday, June 26, 2013 5:56 PM
To: Park, Todd; Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Cc: Khalid, Aryana C. (CMS/OA)
Subject: Re: Follow-up

Thanks Todd. Appreciate the help as always!!!!

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, June 26, 2013 05:34 PM
To: Tavener, Marilyn (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Follow-up

Hi Marilyn, Michelle, and Henry,

After talking with Henry and team, I spoke with Mark about the logo issue, and explained why attempting to add logos for October 1 is extremely unwise. He understands. He may want me to get on the phone with someone from the Blues so they fully understand it. I'm more than happy to do so on your behalf - this issue should not consume any more of your time.

Marilyn, I'm also going to visit with Henry and team for one of our evening deep-dive sessions to get up to speed on the latest status of IT and testing during the week of July 8. Michelle, Henry, and I had a check-in call today, but I think that Henry is right that to really understand current status and next steps, there is no substitute for an evening deep-dive. So I'll bring healthy food and snacks to Baltimore and camp out with Henry and team for a few hours ☺

All the best,
Todd

The right way to add logos to the FFM would be to modify the core plan data submission/management process and systems to include logos as part of the carrier plan/product template and be able to process logos all the way through. This is not doable for Oct 1 without introducing significant operational risk to the go-live, as discussed above. We suggest considering it as part of a future release, post October 1 understanding that it will have to compete with a lot of priorities. The reasonable thing to do would be to target making this modification in time for the next cycle of plan bids, in 2014.

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Tuesday, June 25, 2013 5:48 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Subject: RE: Draft writeup

Looks good.....

A. Michelle Snyder
Deputy Chief Operating Officer
DHHS/CMS
[REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, June 25, 2013 1:13 AM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Draft writeup

Please keep close hold loop in folks who can help with the details, but don't circulate broadly yet, if you don't mind. Let me know if this sounds right any corrections/edits/additions/deletions welcome:

Attempting to integrate logos into the FFM for October 1 is not advisable. This is not because the act of integrating a logo is by itself a difficult thing to do. It's because the process for collecting health plan and product data from carriers via templates, loading these data into the HIOS system, validating the data, transferring the data from HIOS into the FFM QHP database, and having the rating engine retrieve and render that data in the FFM has been locked down, and is being utilized to support plan data collection/validation and system testing as we speak. Changing the underlying plan data template and processing routine right now -- by adding a new plan data element, the logo -- during the crunch-time sprint we're in from now to October 1, would introduce significant risk. Think of it as trying to change a gear in an airplane engine in mid-flight. Or adding a new field to an IRS tax form in the middle of filing season. As an isolated act, adding the field isn't hard. What's hard is the notion of adding it to the tax form via a system modification when that system is going through an intense time, with a lot of moving parts involved, and where a wrong move could actually screw the whole system up.

An alternative to changing the core plan data submission/management process and systems (i.e., modifying the carrier plan data templates, HIOS, the QHP database, and rating engine logic) would be to set up a database of logos outside this core data management process and have the FFM system, when rendering a given insurance product, pull from both the QHP database plus the logo database. This is a terrible idea technically, would be prone to error, and still creates the issue of mucking with the jet engine while it's in flight.

The right way to add logos to the FFM would be to modify the core plan data submission/management process and systems to include logos as part of the carrier plan/product template and be able to process logos all the way through. This is not doable for Oct 1 without introducing significant operational risk to the go-live, as discussed above. We suggest considering it as part of a future release, post October 1 understanding that it will have to compete with a lot of priorities. The reasonable thing to do would be to target making this modification in time for the next cycle of plan bids, in 2014.

From: Jennings, Christopher
Sent: Wednesday, July 17, 2013 8:33 PM
To: Park, Todd; Childress, Mark; marilyn.tavanner; [REDACTED]; Lambrew, Jeanne
Subject: RE: BCBSA conversation update

Thanks Todd. This is helpful information for me to know because the plans are always appealing things. Having said, as per usual, your standing with these folks goes a long way to acceptance. Look forward to getting together. You will be hearing from me to get on your schedule shortly. Thanks for all.

Chris

From: Park, Todd
Sent: Wednesday, July 17, 2013 7:44 PM
To: Childress, Mark; marilyn.tavanner; [REDACTED]; Lambrew, Jeanne; Jennings, Christopher
Subject: BCBSA conversation update

Hi Mark, Marilyn, Jeanne, and Chris,

Spoke with BCBSA this morning - Justine Handelman, Bill O'Loughlin, and Jeannette Ekh.

Was a very good conversation. I explained that we were 100% supportive of adding logos, but that doing so for October 1 was very-high-risk, and explained why in detail. They said that they understood and they very much understood the importance of focusing on mission-critical, core operational execution to support a successful October 1 go-live, which is in everyone's best interest.

They asked about whether logos might be doable for Nov or Dec. I said that we could definitely do logos for the next cycle of plan bids and data submission in 2014 (March 2014 notice; QHP data submission in June/July 2014), and that this would be the logical time to do it. Doing logos before then would require out-of-cycle plan data submission/validation/retrieval/presentation work, and furthermore, that we should expect Oct 2013-Jan 2014 to be a very, very busy time as we execute improvements to the core operation based on what we learn post go-live and as we develop, test, and deploy back-end modules to power financial management and plan payment beginning in Jan 2014.

It sounded like they understood this as well. They appreciated that we were very supportive of doing logos, and appreciated the need to focus on core ops/IT execution in the near-term.

As we discussed, I interwove into the discussion our desire to start ongoing dialogue between CMS and issuer ops/tech people ASAP, to coordinate, test, and prep for Oct 1. I also said that we were very supportive of the idea of having issuer tiger teams and our Marketplace Ops Center collaborate closely on and post Oct 1 which would be a natural outgrowth of the CMS-issuer ops dialogue we start now.

They were very enthusiastic about this, and said that it closely mirrored their own thinking as well - they have actually worked on recommendations for how to proceed with issuer-CMS op/tech collaboration, which they'll be sending to CMS shortly. I said that CMS would be reaching out to issuers ASAP as well. They said that getting started "tomorrow" with ops/tech dialogue would be great, that this collaboration would be a key success factor, and that we're all on the same team.

They'll report back to their board on the logo issue - and will also let the board know about our desire to engage in ongoing collaborative ops/tech dialogue and work. They said that their board would be super-supportive of engaging

They were very enthusiastic about this, and said that it closely mirrored their own thinking as well — they have actually worked on recommendations for how to proceed with issuer-CMS op/tech collaboration, which they'll be sending to CMS shortly. I said that CMS would be reaching out to issuers ASAP as well. They said that getting started "tomorrow" with ops/tech dialogue would be great, that this collaboration would be a key success factor, and that we're all on the same team.

They'll report back to their board on the logo issue — and will also let the board know about our desire to engage in ongoing collaborative ops/tech dialogue and work. They said that their board would be super-supportive of engaging asap in closer dialogue/collaboration. Hopefully, the board will understand what's logical to do with logos as well. Justine and team said that they would articulate the context and explanation, and said that they thought the board would understand the need to focus on mission-critical work in the near-term.

Please let me know if you have any questions!

Cheers,
Todd

From: Childress, Mark
Sent: Wednesday, July 17, 2013 10:34 PM
To: Park, Todd; 'marilyn.tavener'; Lambrew, Jeanne; Jennings, Christopher
Subject: Re: BCBSA conversation update

Thx v much for doing that todd

From: Park, Todd
Sent: Wednesday, July 17, 2013 07:44 PM
To: Childress, Mark; 'marilyn.tavener'; <>; Lambrew, Jeanne; Jennings, Christopher
Subject: BCBSA conversation update

Hi Mark, Marilyn, Jeanne, and Chris,

Spoke with BCBSA this morning Justine Handelman, Bill O'Loughlin, and Jeannette Ekh.

Was a very good conversation. I explained that we were 100% supportive of adding logos, but that doing so for October 1 was very-high-risk, and explained why in detail. They said that they understood and they very much understood the importance of focusing on mission-critical, core operational execution to support a successful October 1 go-live, which is in everyone's best interest.

They asked about whether logos might be doable for Nov or Dec. I said that we could definitely do logos for the next cycle of plan bids and data submission in 2014 (March 2014 notice, QHP data submission in June/July 2014), and that this would be the logical time to do it. Doing logos before then would require out-of-cycle plan data submission/validation/retrieval/presentation work, and furthermore, that we should expect Oct 2013 -Jan 2014 to be a very, very busy time as we execute improvements to the core operation based on what we learn post go-live and as we develop, test, and deploy back-end modules to power financial management and plan payment beginning in Jan 2014.

It sounded like they understood this as well. They appreciated that we were very supportive of doing logos, and appreciated the need to focus on core ops/IT execution in the near-term.

As we discussed, I interwove into the discussion our desire to start ongoing dialogue between CMS and issuer ops/tech people ASAP, to coordinate, test, and prep for Oct 1. I also said that we were very supportive of the idea of having issuer tiger teams and our Marketplace Ops Center collaborate closely on and post Oct 1, which would be a natural outgrowth of the CMS-issuer ops dialogue we start now.

They were very enthusiastic about this, and said that it closely mirrored their own thinking as well. They have actually worked on recommendations for how to proceed with issuer-CMS op/tech collaboration, which they'll be sending to CMS shortly. I said that CMS would be reaching out to issuers ASAP as well. They said that getting started "tomorrow" with ops/tech dialogue would be great, that this collaboration would be a key success factor, and that we're all on the same team.

They'll report back to their board on the logo issue - and will also let the board know about our desire to engage in ongoing collaborative ops/tech dialogue and work. They said that their board would be super-supportive of engaging asap in closer dialogue/collaboration. Hopefully, the board will understand what's logical to do with logos as well. Justine and team said that they would articulate the context and explanation, and said that they thought the board would understand the need to focus on mission-critical work in the near-term.

From: Park, Todd
Sent: Sunday, July 21, 2013 7:10 PM
To: 'Justine.Handelman [mailto: [REDACTED]]'
Cc: 'mara.baer [mailto: [REDACTED]]'; 'Marilyn.Tavener [mailto: [REDACTED]]'; 'Aryana.Khalid [mailto: [REDACTED]]'; Graubard, Vivian; Paris, Randy
Subject: Re: Thanks and Follow-Up

Hi Justine, it was terrific speaking with you and team, and am looping Marilyn and Aryana on the next steps below. -- they have been working on the plan to amp-up technical and operational collaboration between CMS and issuers, which we all agree strongly will be key to success in the lead-up to Oct 1 and beyond.

Marilyn/Aryana, I don't want to be a scheduling bottleneck, as time is of the essence, but would be delighted to participate in any key planning calls for the next phase of work. (Randy/Vivian, cc: d, manage my schedule, and your office can reach out to them anytime -- and again, please don't let me be a bottleneck!)

All the best, and go team go!
Todd

From: Handelman, Justine [mailto: [REDACTED]]
Sent: Sunday, July 21, 2013 11:36 AM
To: Park, Todd
Cc: Baer, Mara <[REDACTED]>
Subject: Thanks and Follow-Up

Todd,

Thanks so much for the call last week. As we shared, logos are a top priority for our Plans because we know how important it will be for consumer shopping but we understand the constraints you are under given all that has to get done before open enrollment.

As we discussed, Plans are working very hard to be ready day 1 but that is only possible if we can be in complete sync with the federal government which will require an open process of sharing operational timelines and detailed operations/IT plans with the issuer community. We are in very close contact with all the CMS staff working on implementation and are currently developing a detailed list of what we need from the agencies to make sure we're all prepared. We would like to share that information with you as well and continue a dialogue about how we work together.

We appreciated hearing about the plans being put together quickly for regular meetings with Administration and Plan technical people to ensure readiness for Oct 1st as well as the "tiger teams" and operations center being developed. Plans are very eager to hear more about these efforts so they can shore up their operations, systems and staffs to be ready. Perhaps we can schedule a call soon to hear more about these activities and timing for plan engagement?

Thanks so much,

Justine

Exhibit 10

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Saturday, August 24, 2013 3:57 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Kerr, James T. (CMS/CMHPO); Outerbridge, Monique (CMS/OIS)
Subject: Re: Additional surges?

We have added some folks and are making arrangements to add others as needed. We need to approach this in a very controlled fashion and not overwhelm CGI or QSSI. On Monday we are walking through the assessment as a result of the thursday through sunday reviews

No further resource action at this time

Thanks

Michelle

Sent from my BlackBerry Wireless Device

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, August 24, 2013 02:38 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Cc: Kerr, James T. (CMS/CMHPO); Outerbridge, Monique (CMS/OIS)
Subject: Additional surges?

Also, Michelle and Henry -- are there any other resource "surges" like the Red Hat surge that you would like to make happen, drawing in additional resources from contractors/subcontractors or Federal employee detailees from other agencies (e.g., Presidential Innovation Fellow developers who could be detailed quickly to CMS)? In the spirit of throwing absolutely everything the US Government can into the fight, please let me know if there is any other surge that you'd like to make happen -- anything at all that could be helpful! Email or call me anytime -- weekend and evenings included, 24-7, at [REDACTED]

Todd

From: Park, Todd
Sent: Friday, August 23, 2013 03:37 PM
To: Chao, Henry (CMS/OIS) <[REDACTED]>; Graubard, Vivian; Mielke, Dawn M.
Cc: Snyder, Michelle (CMS/OA) <[REDACTED]>; Kerr, James T. (CMS/CMHPO)
 <[REDACTED]>; Outerbridge, Monique (CMS/OIS) <[REDACTED]>
Subject: RE: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Henry, you did a terrific job on the call and conceiving this whole Red Hat surge play. Viva la developer surge!! It sounds like Red Hat is really going to lock in and deliver the goods please keep me posted regarding the actual materialization of the surge and if I should call Red Hat to keep applying pressure. Also, as we all discussed, please let me know if I need to talk with other folks across government to explain why their best Red Hat developers are moving immediately to the Marketplace project ☺

Great job, go team go, and semper fi,
Todd

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Friday, August 23, 2013 2:38 PM
To: Park, Todd; Graubard, Vivian; Mielke, Dawn M.
Cc: Snyder, Michelle (CMS/OA); Kerr, James T. (CMS/CMHPO); Outerbridge, Monique (CMS/OIS)
Subject: RE: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

yup

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Park, Todd [mailto:]
Sent: Friday, August 23, 2013 2:37 PM
To: Chao, Henry (CMS/OIS); Graubard, Vivian; Mielke, Dawn M.
Cc: Snyder, Michelle (CMS/OA); Kerr, James T. (CMS/CMHPO); Outerbridge, Monique (CMS/OIS)
Subject: RE: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

OK, terrific. Will they have the slides? And will you lead the talkthrough of the slides?

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Friday, August 23, 2013 2:36 PM
To: Park, Todd; Graubard, Vivian; Mielke, Dawn M.
Cc: Snyder, Michelle (CMS/OA); Kerr, James T. (CMS/CMHPO); Outerbridge, Monique (CMS/OIS)
Subject: FW: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates
Importance: High

This is what we will use for discussion points. Red Hat execs are available at 3pm. QSSI and CGI will both be on the call along with me.

Appoint is coming in a few min.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Kartori Kim [mailto:]
Sent: Friday, August 23, 2013 2:21 PM
To: Chao, Henry (CMS/OIS); Sharma, Hemant (CGI Federal); Campbell, Cheryl (CGI Federal); Martin, Rich (CGI Federal);

Manambedu, Lakshmi (CGI Federal)
Cc: Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS)
Subject: Re: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Karlon Kim
Sr. Vice President of Program Delivery
10480 Little Patuxent Parkway, Suite 1100, Columbia MD 21044
Office [redacted] | mobile [redacted]

From: Karlon Kim <[redacted]>
Date: Friday, August 23, 2013 2:19 PM
To: "henry.chao" <[redacted]>, Hemant Sharma <[redacted]>
"Campbell, Cheryl (CGI Federal)" <[redacted]>, Rich Martin <[redacted]>
"lakshmi.manambedu" <[redacted]>
Cc: Monique Outerbridge <[redacted]>, Mark Oh <[redacted]>
Subject: Re: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

This is where I'm going with it. Haven't received the RedHat execs yet.

Karlon Kim
Sr. Vice President of Program Delivery
10480 Little Patuxent Parkway, Suite 1100, Columbia MD 21044
Office [redacted] | mobile [redacted]

From: <Chao>, "henry.chao" <[redacted]>
Date: Friday, August 23, 2013 2:06 PM
To: Karlon Kim <[redacted]>, Hemant Sharma <[redacted]>, "Campbell, Cheryl (CGI Federal)" <[redacted]>, Rich Martin <[redacted]>
"lakshmi.manambedu" <[redacted]>
Cc: Monique Outerbridge <[redacted]>, Mark Oh <[redacted]>
Subject: RE: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Is it soup yet?

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Karlon Kim [mailto:[redacted]]
Sent: Friday, August 23, 2013 1:06 PM
To: Chao, Henry (CMS/OIS); Sharma, Hemant (CGI Federal); Campbell, Cheryl (CGI Federal); Martin, Rich (CGI Federal); Manambedu, Lakshmi (CGI Federal)
Cc: Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS)

Subject: Re: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates
Importance: High

OK,

Karlton Kim
Sr. Vice President of Program Delivery
10480 Little Patuxent Parkway, Suite 1100, Columbia MD 21044
Office [redacted] | mobile [redacted]

From: <Chao>, "Henry Chao" <[redacted]>
Date: Friday, August 23, 2013 1:00 PM
To: Karlton Kim <[redacted]>, Hemant Sharma <[redacted]>, "Campbell, Cheryl (CGI Federal)" <[redacted]>, Rich Martin <[redacted]>, "lakshmi.manambedu" <[redacted]>
Cc: Monique Outerbridge <[redacted]>, Mark Oh <[redacted]>
Subject: RE: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Karlton,

Please take what Hemant has put together as a single set of skills and delineate between what skills are needed by each side and put that in an agenda/talking points for todd and I the call at 3pm. Need the names of the Red hat execs. too

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Karlton Kim [mailto:[redacted]]
Sent: Friday, August 23, 2013 12:53 PM
To: Sharma, Hemant (CGI Federal); Chao, Henry (CMS/OIS); Campbell, Cheryl (CGI Federal); Martin, Rich (CGI Federal); Manambedu, Lakshmi (CGI Federal)
Cc: Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS)
Subject: Re: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Yes, I will have the dial in, and I will add anything additional we may have to your list

Karlton Kim
Sr. Vice President of Program Delivery
10480 Little Patuxent Parkway, Suite 1100, Columbia MD 21044
Office [redacted] | mobile [redacted]

From: <Sharma>, Hemant Sharma <[redacted]>
Date: Friday, August 23, 2013 12:47 PM
To: Karlton Kim <[redacted]>, "Henry Chao" <[redacted]>, "Campbell, Cheryl (CGI Federal)" <[redacted]>, Rich Martin <[redacted]>

"lakshmi.manambedu [REDACTED]
 cc: Monique Outerbridge <[REDACTED]>, Mark Oh <[REDACTED]>
 Subject: RE: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Hi Henry,

Here is what we can use help with from Red Hat:

1. Java Enterprise (JEE) architects/developers (4 resources) - the expectation is for these resources to be part of a SWAT team to help with:
 - a. Analysis/identification, debugging, and resolution of issues related to FFM application design - one recent example is session management that Mark White from RedHat is helping with.
 - b. Since these are JEE architects/developers they will also help with development activities within the various teams. Resources that have experience with user interface development especially Javascript/Backbone would be very helpful for example resources like Trevor Quinn from RedHat.
2. JBoss SOA-P Performance Tuning (2 resources) - the expectation is that these resources will help with the identification and resolution of issues related to JBoss SOA -P performance and scalability.
3. JBoss Operations (1 resource) - the expectation is that this resource will help with operations and administration related activities of the JBoss middleware infrastructure: such as shell scripting to automate administration/monitoring tasks and experience with JBoss Operations Network. One example resource from RedHat in this category is Ovidiu Fedorov.

Karlton, not sure if you are looking for similar resources, but am guessing there will be some overlap. Let me know if you would like to talk realtime. Also, seems like you have the RedHat contact identified and I don't need to get a different name.

Thanks,
 Hemant

Hemant Sharma | Vice President, CGI Federal | 12601 Fair Lakes Circle, VA, 22033 | Office [REDACTED] | Mobile [REDACTED]
www.cgi.com

CONFIDENTIALITY NOTICE: Proprietary/Confidential information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message, and are asked to notify the sender by reply email.

From: Karlton Kim [mailto:[REDACTED]]
 Sent: Friday, August 23, 2013 11:25 AM
 To: Chao, Henry (CMS/OIS); Campbell, Cheryl (CGI Federal); Martin, Rich (CGI Federal); Sharma, Hemant (CGI Federal); Manambedu, Lakshmi (CGI Federal)
 Cc: Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS)
 Subject: Re: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates
 Importance: High

Yes. We will give you skill set / expertise.

Karlton Kim
 Sr. Vice President of Program Delivery
 10480 Little Patuxent Parkway, Suite 1100, Columbia MD 21044
 Office [REDACTED] | mobile [REDACTED]

From: <Chao>, "Henry Chao" <[REDACTED]>
Date: Friday, August 23, 2013 11:21 AM
To: Kariton Kim <[REDACTED]>, "Campbell, Cheryl (CGI Federal)" <[REDACTED]>, Rich Martin <[REDACTED]>, Hemant Sharma <[REDACTED]>, "lakshmi.manambedu" <[REDACTED]>
Cc: Monique Outerbridge <[REDACTED]>, Mark Oh <[REDACTED]>
Subject: Recruiting a top notch Red Hat team to assist in the Pods to ensure quality and ability to meet targeted dates

Todd Park requested that we provide him the right contact at Red Hat so he can request Red Hat to provide their top hands-on experts (Developers, Engineers, Testers, Performance, Architects, troubleshooters, etc.) to our CGI and QSSI vehicles. We already have a few really good people and we can benefit from this offer to round up more of the best to work with us.

Here's what I need:

Hemant and Kariton please list the skillsets you believe we have a gap in or need more of for Red Hat at the level of expertise greater than what we currently have access to. Also talk to your Red Hat Contacts to get the right executive listed on the following page for Todd to call (and ask your Red Hat contact for the information for Todd.

<http://www.redhat.com/about/company/management/>

Please get that back to me before 3pm. Does that work?

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

Exhibit 11

From: Fasching, Laura <[REDACTED]>
 Sent: Sunday, September 29, 2013 1:53 AM
 To: Park, Todd; 'henry.chao' <[REDACTED]>
 Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Understood and I will call you if we hit a snag .
 Thanks

-----Original Message-----

From: Park, Todd [mailto:[REDACTED]]
 Sent: Sunday, September 29, 2013 01:47 AM Eastern Standard Time
 To: Fasching, Laura; 'henry.chao' <[REDACTED]>
 Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Laura, terrific, thanks! If you run into issues, no matter what hour it is, please call me at [REDACTED] -- my phone will be on and next to my ear all night; please don't hesitate to call at any hour. And we can trigger the backup option at literally any hour of the night if need be.

Thanks!
 Todd

From: Fasching, Laura [mailto:[REDACTED]]
 Sent: Sunday, September 29, 2013 01:25 AM
 To: Park, Todd; 'henry.chao' <[REDACTED]>
 Cc: Fasching, Laura <[REDACTED]>
 Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Ok thanks Todd, we are good for now the shippers are at the data center getting ready to pick up the gear now. We will let you know if we run into any issues and need the back up options.
 Thanks
 Laura

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: [REDACTED]
 222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
 Sent: Sunday, September 29, 2013 12:08 AM
 To: Fasching, Laura; 'henry.chao' <[REDACTED]>
 Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Laura, can you let us know when the shippers do indeed pick up the equipment from Miami and that the private cargo transport play is officially in motion and good to go?

We in fact have ascertained that military transport is available as a backup option in case the commercial option falls through at the last second -- but the commercial option is more cost-effective. However, if the commercial shippers

flake out, we can activate the military option -- folks are standing by.

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 10:46 PM
To: Park, Todd; Chao, Henry (CMS/OIS) < >
Cc: Fasching, Laura < >
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Glad to help, let me know if you need anything else gentlemen ☺
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel:
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:]
Sent: Saturday, September 28, 2013 10:38 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

That is super-awesome Laura, thanks so very, very, very much!!!!

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 10:36 PM
To: Chao, Henry (CMS/OIS); Park, Todd
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd & Henry,

The shipper is picking up the equipment in the next 90 minutes from the Miami data center and we expect the shipment to arrive between 9:30 AM to 10:00 AM. ☺

So Monday COB is looking good as long as we keep the shippers on schedule, as the build teams will be working at 6 am with the equipment that was brought in today.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel:
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Saturday, September 28, 2013 9:03 PM
To: Fasching, Laura; Todd Y Park
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

I got the approval from our COO and head of Contracts to go with the 40k option.

Contracts said we will have to work out how this can be a line you can bill in the contract but no problem figuring that out later.

Henry Chao
 Deputy Chief Information Officer and Deputy Director
 Office of Information Services
 Centers for Medicare & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 09:00 PM
To: Park, Todd < >; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura < >
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Ok great Henry can I get confirmation that the Government will pay for the plane? We have to get David Small's approval so we will need to call him as soon as possible.

Thanks and sorry to rush you all.

Laura

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: 214.241.2244
 222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:]
Sent: Saturday, September 28, 2013 8:50 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

FYI, the private plane option I am pursuing would likely cost about the same as the FedEx expedite cargo plane option below.

Henry, I think that delivery to the data center mid-day Sunday sounds really, really, really good...

From: Fasching, Laura [mailto:]
Sent: Saturday, September 28, 2013 8:46 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?
Importance: High

Ok here is what I was able to do
 I was able to get to FedEx custom Critical they can drive it to us via a truck with pick up tonight @ 11:00 PM (ish) and delivery around 9 PM on Sunday night for \$3700.00

Or
 They have an expedite cargo plane option which would get all 6 pallets on the plane (insured/ bonded) and get the delivery to the data center by mid-day Sunday which still gives us a good amount of time to work on the configurations. The cost however is \$40,000.00.

if you would want to move on either of these options let me know as we need Henry to approve the costs.

Thanks
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 8:37 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

OK, have reached a private plane broker. They are investigating ASAP. I told them Miami to Dulles was the desired flight path is that correct?

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 8:10 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Quantity 6 200.00 lb pallets Dimensions: 39x25x33

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 7:58 PM
To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

OK you can call me at [REDACTED] or [REDACTED]

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 7:57 PM
To: 'laura.fasching@[REDACTED]'; Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper ?

I'll call and patch you both in

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244
[REDACTED] (Pri)

[Redacted] (Alt)
[Redacted] (BB)

From: Fasching, Laura [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 07:56 PM
To: Park, Todd <[Redacted]>; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura <[Redacted]>
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

[Redacted] I am available of course ☺

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [Redacted]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 7:55 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Hi Laura, can you get on the phone for a moment to discuss? What's the best number at which to reach you?

From: Fasching, Laura [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 7:53 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Ok I have confirmed our Air force option is a go and is the best option as we will have the build resources available for the full build and be able to deliver that on Monday

We are working with trucking companies now to get a truck to pick up sometime tomorrow and direct ship it to us again the equipment would not get here until Monday morning at the earliest and then you're looking at Wednesday/Thursday delivery and at that point we should go with our original shipping plan.

And lastly we are having a challenge on getting the logistics aligned for a chartered cargo plane, it looks like we may not be able to get that arranged until Monday morning and would not know until then when they could pick & deliver the equipment --so this option would need to be explored in depth on Monday.

This is what we have at this point.
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [Redacted]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[Redacted]]
Sent: Saturday, September 28, 2013 7:34 PM
To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Laura, by when do you need to make a decision about whether to send via private ground, private cargo plane, or Air Force (if Air Force is indeed an option?)

And to confirm private ground would deliver the hardware on Tuesday (to be installed Wednesday?), private cargo plane would deliver the hardware on Monday (to be installed Tuesday?). With no possibility of acceleration of those timetables?

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 7:29 PM
To: 'laura.fasching@ [REDACTED]'; Park, Todd
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd--it's in your hands now to make a quick decision.

Henry Chao
 Deputy Chief Information Officer and Deputy Director
 Office of Information Services
 Centers for Medicare & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244

From: Fasching, Laura [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 07:27 PM
To: Park, Todd < [REDACTED] >; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

We have been exploring that option too but no luck so far

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: [REDACTED]
 222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 7:26 PM
To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Also: as another option to explore, in the interest of exploring all options simultaneously, is it possible to arrange for heroic chartered private sector ground transportation that could get going super-early tomorrow morning and get to Culpeper by Sunday evening?

From: Park, Todd
Sent: Saturday, September 28, 2013 7:03 PM
To: 'Chao, Henry (CMS/OIS)'; 'laura.fasching@ [REDACTED]'
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

WH team responded instantly, is working on it as we speak and will get back to us ASAP. But they unfortunately are not optimistic, so we should explore other options in parallel.

Is there any possibility of arranging for private/commercial cargo plane transport? Chartered, even?

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 6:36 PM
To: 'laura.fasching@verizon.com' [mailto: [REDACTED]]
Cc: Park, Todd
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Just talked to Todd and he is going to talk to the rest of WH that can make this happen so just reply with the confirmed service to Homestead.

Todd--let us know ASAP so laura will send via ground if you can't arrange for transport to someplace the Air Force can land near Culpeper VA.

Henry Chao
 Deputy Chief Information Officer and Deputy Director
 Office of Information Services
 Centers for Medicare & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244

[REDACTED]
 [REDACTED]
 [REDACTED]

From: Fasching, Laura [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 06:09 PM
To: Chao, Henry (CMS/OIS)
Cc: Fasching, Laura < [REDACTED] >
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Henry,

We are working on firming up the white glove shippers but once that is done we would be good to go.

If we get the shippers scheduled and the equipment gets here tomorrow my engineers said they have the resources to build it out and just like we said before up by cob Monday.

I will let you know about the shippers within an hour.

Laura

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: [REDACTED]
 222 W Las Colinas Blvd, Irving, Texas, 75039

From: Fasching, Laura
Sent: Saturday, September 28, 2013 5:27 PM
To: Chao, Henry (CMS/OIS)

Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Henry,

If you can make it happen wow

The equipment would be

Below is the possible weight, quantity, and size of the pending shipment.
Quantity 6 200.00 lb pallets. Dimensions 39x25x33

On our side we have to get the equipment from the data center to Homestead AFB so I have the team looking at white glove courier services now. We would use the same kind of service to pick up the gear at Andrews Air Force base and have them transport it to Culpeper.

While they look for the white glove courier, I will make sure engineering will be able to add this space to their work load to have it over to you on Monday with the rest of the compute.

I am on calls with folks now to firm up our ability to pull off the logistics on our side, I will update you shortly.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

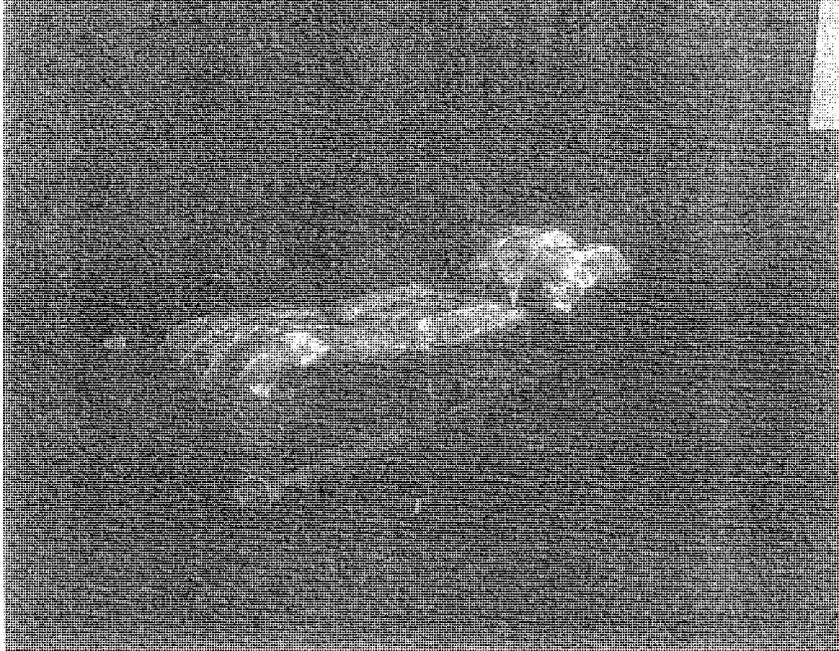
From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 4:56 PM
To: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?
Importance: High

Todd Park is willing to ask if we can define the need so that means to me if we can get the AF involved we would target tomorrow morning to get the equipment installed at Culpeper before 10/1.

Let me know

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Chao, Henry (CMS/OIS)
Sent: Saturday, September 28, 2013 4:54 PM
To: Fasching, Laura ([REDACTED])
Subject: How serious are you about using Homestead AFB to get the equipment to Culpeper?
Importance: High



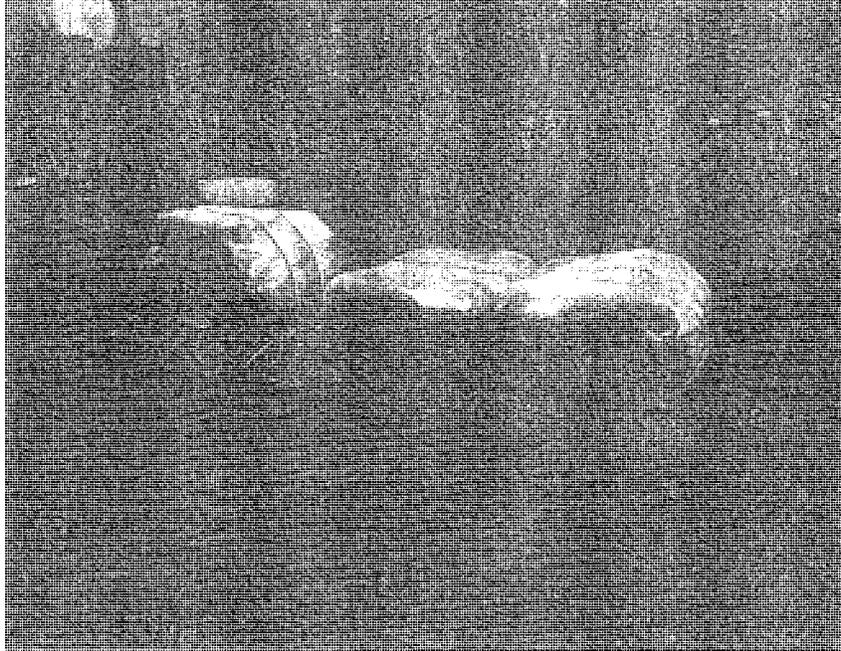


Exhibit 12

From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Friday, August 23, 2013 6:35 PM
To: Park, Todd; Snyder, Michelle (CMS/OA)
Subject: RE: Response to Todd's Cybersecurity bullet requests.

Michelle beat me to it.

From: Park, Todd [mailto:[REDACTED]]
Sent: Friday, August 23, 2013 6:34 PM
To: Snyder, Michelle (CMS/OA)
Cc: Trenkle, Tony (CMS/OIS)
Subject: RE: Response to Todd's Cybersecurity bullet requests.

I think these are great - thank you. Will send to Marilyn/Jeanne, and cc: the two of you + Frank Baitman, as Tony suggests. Thanks again!

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]
Sent: Friday, August 23, 2013 6:21 PM
To: Park, Todd
Subject: Fw: Response to Todd's Cybersecurity bullet requests.
Importance: High

Here they are.

Sent from my BlackBerry Wireless Device

From: Trenkle, Tony (CMS/OIS)
Sent: Friday, August 23, 2013 04:52 PM
To: Snyder, Michelle (CMS/OA)
Cc: Chao, Henry (CMS/OIS); King, Terris (CMS/OIS); Trenkle, Tony (CMS/OIS)
Subject: Response to Todd's Cybersecurity bullet requests.

Michelle,

Below are the bullets that I suggest that we send to Todd. We kept them focused on CMS and fairly generic. I can forward them to Todd or you can. We can also add to them if you want any statistics etc. Also, we should probably copy Frank on the response in case he wants to add anything from the HHS perspective:

- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.
- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which

From: Park, Todd
Sent: Friday, August 23, 2013 6:45 PM
To: marilyn.tavener; Lambrew, Jeanne
Cc: michelle.snyder; Trenkle, Tony (CMS/OIS); frank.baitman
Subject: Cybersecurity bullet points

Hi Jeanne and Marilyn, here are bullet points from Team CMS about how the Marketplace will be protected from cyber-attacks. Folks can add statistics and other additional info if desired. Also looping Frank Baitman from HHS.

- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.
- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

From: Park, Todd [mailto:]
Sent: Friday, August 23, 2013 11:14 AM
To: Snyder, Michelle (CMS/OA); Trenkle, Tony (CMS/OIS)
Cc: Taverner, Marilyn (CMS/OA)
Subject: Cybersecurity bullet points needed
Importance: High

Hi Michelle and Tony, Marilyn/WH folks would love to get three basic bullet points describing how we will protect the Marketplace from cyberattack. Many apologies, but if we could get these by COB today, that would be fantastic is that possible?

Below are three strawcase bullet points folks have drafted feel free to edit/change in any way you see fit. See notes following each bullet as well.

• The Center for Medicare and Medicaid Services (CMS) and the Internal Revenue Service (IRS) have been relentlessly attacked, given the amount of funding that they manage, yet there has never been a major breach and loss of personally identifiable information or loss of taxpayer dollars. NOTE: want to make sure this is stated/framed accurately.

• The use of electronic applications does not necessarily make information less secure. For example, in 2012, 119 million taxpayers filed electronically, with less than half a million fraction being affected by identify theft since 2008. NOTE: you may want to replace this bullet entirely with another bullet that describes CMS's cybersecurity approach and capabilities. If you want to add more than one bullet on that, that's also totally cool.

• The information technology systems that are being created for the Marketplace meet or exceed existing government standards. In addition, HHS is working with States, IRS, DOJ and the FTC on a comprehensive plan to identify, prevent, detect, and prosecute identify theft and fraud.

Thanks so very, very much for your help,

Todd

Exhibit 13

From: Park, Todd
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: michelle.snyder; [REDACTED]; Mielke, Dawn M.; Gräubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later - looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others - we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace - we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Wednesday, August 28, 2013 9:52 AM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS)
Subject: Re: Cyber next steps

Todd

Yes, this is consistent with what we discussed yesterday. Looping in Frank and Teresa.

Michelle

I assume that we should have Henry there as well.

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, August 28, 2013 09:44 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M. <[REDACTED]>; Graubard, Vivian <[REDACTED]>
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later. Looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well; FYI for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace -- we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
 Todd

From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OIG)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later. Looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others - we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, but for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace - we should do a confidential, cone of silence. consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
 Todd

From: Park, Todd
Sent: Wednesday, August 28, 2013 6:45 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO); Khaïd, Aryana C. (CMS/OA)
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo - will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
 Todd

From: Trenkle, Tony (CMS/OIS) [mailto:████████████████████]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:████████████████████]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. We should convene a work session in the next week with you, Teresa, Frank Bait man, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later. Looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace – we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!

Todd

From: Trenkle, Tony (CMS/OIS) <[mailto:]>
Sent: Wednesday, August 28, 2013 7:01 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO); Khalid, Aryana C. (CMS/OA)
Subject: Re: Cyber next steps

Frank

Your call. I can move things around but I thought you were tied up

From: Park, Todd [mailto:]
Sent: Wednesday, August 28, 2013 06:44 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M. <[mailto:]>; Graubard, Vivian <[mailto:]>; Baitman, Frank (OS/ASA/OCIO); Khalid, Aryana C. (CMS/OA)
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check @

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo - will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
 Todd

From: Trenkle, Tony (CMS/OIS) [mailto:]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later - looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others - we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi - for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace - we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

From: Baitman, Frank (OS/ASA/OCCO) <[REDACTED]>
Sent: Wednesday, August 28, 2013 7:24 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCCO/OIS)
Subject: Re: Cyber next steps

+ Adding Kevin

Todd et al,

Unfortunately the Secretary's Leadership Council is next Wed afternoon and believe we'll have some IT items on the agenda, so I need to be there.

I believe we can address our defenses in a balanced manner. It should come as no surprise that we experience attacks and have defenses. But, for public facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage.

- Frank

From: <Park>, Todd <[REDACTED]>
Date: Wednesday, August 28, 2013 6:44 PM
To: "Trenkle, Tony (CMS/OIS)" <[REDACTED]>
Cc: "Snyder, Michelle (CMS/OA)" <[REDACTED]>, "Mielke, Dawn M." <[REDACTED]>, "Graubard, Vivian" <[REDACTED]>, Frank Baitman <[REDACTED]>, "Khalid, Aryana C. (CMS/OA)" <[REDACTED]>
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful :

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
Todd

From: Trenkle, Tony (CMS/OIS) [mailto:]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCL O)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions :

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later. Looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others --- we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace -- we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

From: Park, Todd
Sent: Wednesday, August 28, 2013 7:38 PM
To: Baitman, Frank (OS/ASA/OCIO); Trankle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: RE: Cyber next steps

OK, will try to call in for a 10 am Wed meeting and make that work. And Frank, agree with your points about public-facing material.

Thanks!
 Todd

From: Baitman, Frank (OS/ASA/OCIO) [mailto: [REDACTED]]
Sent: Wednesday, August 28, 2013 7:24 PM
To: Park, Todd; Trankle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cyber next steps

+ Adding Kevin

Todd et al,

Unfortunately the Secretary's Leadership Council is next Wed afternoon and believe we'll have some IT items on the agenda, so I need to be there.

I believe we can address our defenses in a balanced manner. It should come as no surprise that we experience attacks and have defenses. But, for public facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage.

- Frank

From: <Park>, Todd < [REDACTED] >
Date: Wednesday, August 28, 2013 6:44 PM
To: "Trankle, Tony (CMS/OIS)" < [REDACTED] >
Cc: "Snyder, Michelle (CMS/OA)" < [REDACTED] >, "Mielke, Dawn M." < [REDACTED] >, "Graubard, Vivian" < [REDACTED] >, Frank Baitman < [REDACTED] >, "Khalid, Aryana C. (CMS/OA)" < [REDACTED] >
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check. ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo - will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
Todd

From: Trenkle, Tony (CMS/OIS) [mailto:]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCI O)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later - looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others - we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace - we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Wednesday, August 28, 2013 9:37 PM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO); Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cyber next steps

I think that we all can agree on that. Todd, the call will follow the outline that you laid out in your email and our discussion should then drive what we say in the memo.

On Aug 28, 2013, at 7:38 PM, "Park, Todd" <[REDACTED]> wrote:

OK, will try to call in for a 10 am Wed meeting and make that work. And Frank, agree with your points about public-facing material.

Thanks!
 Todd

From: Baitman, Frank (OS/ASA/OCIO) [mailto:[REDACTED]]
Sent: Wednesday, August 28, 2013 7:24 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cyber next steps

+ Adding Kevin

Todd et al,

Unfortunately the Secretary's Leadership Council is next Wed afternoon. and believe we'll have some IT items on the agenda, so I need to be there.

I believe we can address our defenses in a balanced manner. It should come as no surprise that we experience attacks and have defenses. But, for public facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage.

- Frank

From: <Park>, Todd <[REDACTED]>
Date: Wednesday, August 28, 2013 6:44 PM
To: "Trenkle, Tony (CMS/OIS)" <[REDACTED]>
Cc: "Snyder, Michelle (CMS/OA)" <[REDACTED]>; "Mielke, Dawn M." <[REDACTED]>; "Graubard, Vivian" <[REDACTED]>; "Khalid, Aryana C. (CMS/OA)" <[REDACTED]>; "Frank Baitman" <[REDACTED]>
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful :

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo. Will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack; (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
Todd

From: Trenke, Tony (CMS/OIS) [mailto:████████████████████]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:████████████████████]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenke, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions :

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later. Looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!

2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others - we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace - we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

From: Park, Todd
Sent: Wednesday, August 28, 2013 9:40 PM
To: 'tony.trenkle [mailto: [REDACTED]]'
Cc: 'frank.baitman [mailto: [REDACTED]]'; 'Michelle.Snyder [mailto: [REDACTED]]'; Mielke, Dawn M.; Graubard, Vivian; 'Aryana.Khalid [mailto: [REDACTED]]'; 'Kevin.Charest [mailto: [REDACTED]]'
Subject: Re: Cyber next steps

Terrific, Tony, thanks, looking forward to it!

Todd

From: Trenkle, Tony (CMS/OIS) [mailto: [REDACTED]]
Sent: Wednesday, August 28, 2013 09:37 PM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) < [REDACTED] >; Snyder, Michelle (CMS/OA) < [REDACTED] >; Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA) < [REDACTED] >; Charest, Kevin (OS/ASA/OCIO/OIS) < [REDACTED] >
Subject: Re: Cyber next steps

I think that we all can agree on that. Todd, the call will follow the outline that you laid out in your email and our discussion should then drive what we say in the memo.

On Aug 28, 2013, at 7:38 PM, "Park, Todd" < [REDACTED] > wrote:

OK, will try to call in for a 10 am Wed meeting and make that work. And Frank, agree with your points about public-facing material.

Thanks!
 Todd

From: Baitman, Frank (OS/ASA/OCIO) [mailto: [REDACTED]]
Sent: Wednesday, August 28, 2013 7:24 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cyber next steps

+ Adding Kevin

Todd et al,

Unfortunately the Secretary's Leadership Council is next Wed afternoon. and believe we'll have some IT items on the agenda, so I need to be there.

I believe we can address our defenses in a balanced manner. It should come as no surprise that we experience attacks and have defenses. But, for public-facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage.

- Frank

From: <Park>, Todd <[REDACTED]>
Date: Wednesday, August 28, 2013 6:44 PM
To: "Trenkle, Tony (CMS/OIS)" <[REDACTED]>
Cc: "Snyder, Michelle (CMS/OA)" <[REDACTED]>, "Mielke, Dawn M." <[REDACTED]>, "Graubard, Vivian" <[REDACTED]>, Frank Baitman <[REDACTED]>, "Khalid, Aryana C. (CMS/OA)" <[REDACTED]>
Subject: RE: Cyber next steps.

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo - will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
 Todd

From: Trenkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)

Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions :

1. We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later - looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others - we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi - for internal use only.
3. I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace - we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

From: Siskel, Edward
Sent: Thursday, August 29, 2013 11:13 AM - FTC
To: Dotzel, Peggy (HHS/OGC) [REDACTED]; Dori Salcido [REDACTED] - HHS
 Michael Hash [REDACTED] - HHS; Igraismar [REDACTED]; Axelrod, Matthew (ODAG) DOJ
Cc: Jennings, Christopher; Lambrew, Jeanne; McGuinness, Tara; Leinwand, Jessica; Suvor, Daniel; Park, Todd
Subject: Follow up items

Thanks again for participating in yesterday's meeting and for all the work you have been doing to help protect consumers during the roll-out of the Marketplaces. Below is a list of do-outs from the meeting based on my notes. Please let me know if I am missing anything or if you have any questions. We will reconvene the group next week and ideally will have made substantial progress on each of these items by then. Also, I only have email addresses for a few of the participants in yesterday's meeting, so please forward this on to the other representatives from your agencies.

- HHS, HHS OIG and FTC will finalize procedures for referral of consumer fraud complaints through the call center, HHS OIG line, and online (training materials for operators; protocol for live transfers when caller elects; links to FTC website from healthcare.gov and the HHS OIG website).
- HHS and FTC will develop (1) training materials for state-run exchanges to use in their call centers; and (2) a link to be provided to the state-run exchanges to use on their websites.
- FTC will develop an easy "how to" document that explains how to register a complaint (including use of drop-down menu).
- FTC/CMS will follow up with Vicki to incorporate the public education materials that HHS OIG has started to create to develop educational material to consumers who register a complaint.
- FTC will add to DOJ's "track record" document or create a parallel version.
- HHS will continue to refine fact sheets and public education materials and circulate to the group.
- All agencies will explore outside validators who can speak to the relevant issues (public education/outreach, intake process, value of Sentinel, prosecution, etc.).

Thanks, Ed

From: Mary.Horne, [REDACTED] >on behalf of:Trenkle, Tony (CMS/OIS) <[REDACTED]>

To: Park, Todd <[REDACTED]>
[REDACTED] <[REDACTED]>
> Fryer, Teresa M. (CMS/OIS)
> Schankweiler, Thomas W. (CMS/OIS)
> Baitman, Frank (OS/ASA/OCIO)
> Charest, Kevin (OS/ASA/OCIO/OIS)

Cc: Mellor, Michael (CMS/OIS) <[REDACTED]>
> Callaghan, Liz M. (OS/ASA/OCIO)
> Byczkowski, Roxanne (CMS/OIS)
> Mielke, Dawn M.
[REDACTED] <[REDACTED]>
Velasco, Linda J. (CMS/OIS) <[REDACTED]>

Bcc:

Subject: Marketplace Security - WebEx: [REDACTED] (internal); [REDACTED] (external); Mtg. No. [REDACTED]

Date: Fri Aug 30 2013 14:48:43 EDT

Attachments:

The above-subject meeting was requested by Tony Trenkle to occur on this day at this time. If you are unable to attend this meeting, please call the OIS Front Office at [REDACTED].

Meeting Number: [REDACTED]
Meeting Password: This meeting does not require a password.

Audio conference information

1. Please call the following number.
WebEx: [REDACTED]
2. Follow the instructions you hear on the phone.
Your WebEx Meeting Number: [REDACTED]

To join from the Baltimore, Chicago, or Kansas City offices

1. Dial ext. [REDACTED]
2. Enter the Meeting Number: [REDACTED]

To start the online meeting

1. Go to [REDACTED]
2. If you are not logged in, log in to your account.

From: Park, Todd
Sent: Monday, September 02, 2013 12:02 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; Aryana, Khalid [REDACTED];
'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]';
Graubard, Vivian
Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

-- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Park, Todd
 Sent: Monday, September 02, 2013 12:10 PM
 To: 'tony.trenkle'; 'frank.baitman'
 Cc: 'Michelle.Snyder'; Graubard, Vivian; Mielke, Dawn M.
 Subject: A couple of follow-ups

Hi Tony and Frank! A couple of follow-ups to my email to Chris below:

1. Just wanted to make sure that we're going to have DHS and DOI folks on the 10 am call on Wed, as per our original plan?
2. It looks like the call with Alex Karp's top cyber folks will be 4 pm on Wednesday – Tony, can you join this call? Feel free to have others join as well. Frank, I think you may be in a mtg, but if you can join as well, that would be terrific... The agenda would be to (in confidence) discuss our cyber positioning and plans and get their thoughts. Dawn/Viv, can you make sure Tony/Frank are invited? Thanks!

Cheers,
 Todd

----- Original Message -----

From: Park, Todd
 Sent: Monday, September 02, 2013 12:02 PM
 To: Jennings, Christopher
 Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian
 Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday – am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

– The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

– CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

– The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

– Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

– As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts – we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Jennings, Christopher
Sent: Monday, September 02, 2013 12:29 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [REDACTED]. We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd
Sent: Monday, September 02, 2013 12:02 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an

attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

— As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts — we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Baitman, Frank (OS/ASA/OCIO) <[REDACTED]>
Sent: Monday, September 02, 2013 1:21 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cybersecurity points
Importance: High

Looping Kevin into this conversation as well.

I think we can come up with something.

- Frank

On 9/2/13 1:14 PM, "Park, Todd" <[REDACTED]> wrote:

>Hi Tony, many apologies for interrupting your Labor Day, but can you
>help Chris with his follow-up question below (reference to "current
>federal standards and how they exceed private sector as well as track
>record of protection from attacks"). I think the federal standards
>reference may refer to federal privacy/security standards? And with
>respect to track record of protection from attacks, I think a couple of
>sentences of additional description on this front would be sufficient
>(and again, this is for internal purposes, not external communication),
>

>[REDACTED] so getting Chris points by
>tonight would be amazingly helpful, if at all possible -- might this be
>possible? Thanks so very much...

>Todd

>----- Original Message -----

>From: Jennings, Christopher
>Sent: Monday, September 02, 2013 12:28 PM
>To: Park, Todd
>Cc: Lambrew, Jeanne; Jones, Isabel; Aryana, Khalid [REDACTED]
>[REDACTED]; Michelle, Snyder [REDACTED]
>Michelle, Snyder [REDACTED]; tony.trenkle [REDACTED]
>tony.trenkle [REDACTED]; frank.baitman [REDACTED]
>[REDACTED]; Graubard, Vivian
>Subject: RE: Cybersecurity points

>Ok, thanks Todd. Quite helpful and will serve as placeholder for

>[REDACTED]
>[REDACTED] We need to have all of this locked down for September 11th

>hearing; we also have to have strong message with Justice, FTC, HHS and
>others for our enforcement event the week of the 16th. I know we had
>reference somewhere to current federal standards and how they exceed
>private sector as well as track record of protection from attacks. Can
>you or someone provide that reference for me to bolster confidence
>building tomorrow? Thanks much for all. And safe and fun travels my
>friend.

>

>Chris

>

>-----Original Message-----

>From: Park, Todd

>Sent: Monday, September 02, 2013 12:02 PM

>To: Jennings, Christopher

>Cc: Lambrew, Jeanne; Jones, Isabel; Aryana.Khalid [REDACTED]

>Michelle.Snyder [REDACTED]; Tony.Trenkle [REDACTED];

>Frank.Baitman [REDACTED]; Graubard, Vivian

>Subject: Cybersecurity points

>

>Hi Chris, here are cybersecurity background points for [REDACTED]
>[REDACTED]. The first three are the points CMS put
>together previously which I'm sure you've already seen; they are
>followed by a couple of points about next steps currently underway.
>Please let us know if you have any questions. I'll be on a long flight
>for much of Tuesday

>I am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and
>Aryana, who can answer any questions you have that might arise.

>

>The Centers for Medicare and Medicaid Services (CMS) has maintained
>a strong history of preventing major breaches involving the loss of
>personally identifiable information from cyber-attacks. CMS has in
>place established risk management, security controls assessment, and
>security authorization processes for all CMS systems. These controls
>meet or exceed existing Federal standards.

>

>CMS has been an innovator leader in the information security
>community through the use of state of the art continuous monitoring
>tools that remotely scan the IT assets of CMS systems to ensure
>baseline configurations are up to date and compliant and that
>deviations are quickly identified and mitigated. Additionally these
>technologies have the capability to detect unknown or rogue hosts which
>are quickly identified and blocked. Penetration testing is also
>performed on all CMS systems to identify vulnerabilities and reduce or
>eliminate potential risks from external threats.

>

>The IT systems that are being created for the Marketplace will meet
>or exceed existing Federal security standards and will utilize state of
>the art monitoring and surveillance tools. CMS is also working closely
>with HHS and other public and private sector security experts to get
>additional technical support for the Marketplace program.

>

>Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept

>4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for
>and defenses against cyberattack, (2) what our response/action would be
>in the event of an attack/crisis, and (3) how we would prosecute attackers.
>CMS will then produce a memo summarizing the above by the end of the week.
>
>-- As an fyi, we have also reached out to Alex Karp and team. Alex
>put us in touch with his top cyber experts -- we are slated to speak
>with them on Wednesday as well.
>
>Chris, again, please let us know if you have any questions!
>
>All the best,
>Todd

From: Park, Todd
Sent: Monday, September 02, 2013 2:19 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people -- they are tracking folks down today and will seek to get you additional info by tonight... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
 Todd

----- Original Message -----

From: Jennings, Christopher
Sent: Monday, September 02, 2013 12:28 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [REDACTED]. We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

----- Original Message -----

From: Park, Todd
Sent: Monday, September 02, 2013 12:02 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

-- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Jennings, Christopher
Sent: Monday, September 02, 2013 2:43 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

----- Original Message -----

From: Park, Todd
Sent: Monday, September 02, 2013 2:19 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people – they are tracking folks down today and will seek to get you additional info by tonight.... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
Todd

----- Original Message -----

From: Jennings, Christopher
Sent: Monday, September 02, 2013 12:28 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; '<[REDACTED]>'; 'Michelle.Snyder [REDACTED]'; '<[REDACTED]>'; 'tony.trenkle [REDACTED]'; '<[REDACTED]>'; 'frank.baitman [REDACTED]'; '<[REDACTED]>'; Graubard, Vivian
Subject: RE: Cybersecurity points

OK, thanks Todd. Quite helpful and will serve as placeholder for [REDACTED]
[REDACTED] We need to have all of this locked down for September 11th hearing; we also have to have strong

message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 12:02 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; Aryana, Khalid [REDACTED]; Michelle Snyder [REDACTED]

'tony.trenkle [REDACTED]; Frank Baitman [REDACTED]; Graubard, Vivian

Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

-- As an FYI, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,

Todd

From: Park, Todd
Sent: Tuesday, September 03, 2013 1:38 AM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'Frank.Baltman [REDACTED]'; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris, here are an expanded/updated set of bullet points from Frank and Tony:

- Like all publicly facing Internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state of the art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff; when the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Market place program.
- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.
- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US -CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----

From: Jennings, Christopher
Sent: Monday, September 02, 2013 02:43 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]';
'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]';
'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

----- Original Message -----

From: Park, Todd
Sent: Monday, September 02, 2013 2:19 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]';
'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people -- they are tracking folks down today and will seek to get you additional info by tonight.... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
Todd

----- Original Message -----

From: Jennings, Christopher
Sent: Monday, September 02, 2013 12:28 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]';
'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]';
'frank.baitman [REDACTED]'; Graubard, Vivian
Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [REDACTED]. We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from

attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 12:02 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'

'Tony.trenkle [REDACTED]'; 'Frank.Baitman [REDACTED]'; Graubard, Vivian

Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

– The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

– CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

– The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

– Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

– As an FYI, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Jennings, Christopher
Sent: Tuesday, September 03, 2013 7:12 AM
To: Park, Todd; Siskel, Edward
Cc: Lambrew, Jeanne; Jones, Isabel; 'aryana.khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian
Subject: Re: Cybersecurity points

Thank you Todd and all on this email. Very helpful and greatly appreciated. Thanks to all for this background and, more importantly, your great work to protect us from cyber attacks/security threats.

Chris

----- Original Message -----

From: Park, Todd
Sent: Tuesday, September 03, 2013 01:38 AM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'aryana.khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris, here are an expanded/updated set of bullet points from Frank and Tony:

- Like all publicly facing internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state of the art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff: when the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security

standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.

-- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US-CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 02:43 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]';

'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]';

'frank.baitman [REDACTED]'; Graubard, Vivian

Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

----- Original Message -----

From: Park, Todd

Sent: Monday, September 02, 2013 2:19 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]';

'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; Graubard, Vivian

Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people -- they are tracking folks down today and will seek to get you additional info by tonight... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,

Todd

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 12:28 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'frank.baitman [REDACTED]'; 'tony.trenkle [REDACTED]'; 'Graubard, Vivian [REDACTED]'

Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [REDACTED]. We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

----- Original Message -----

From: Park, Todd

Sent: Monday, September 02, 2013 12:02 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; 'Graubard, Vivian [REDACTED]'

Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

371

-- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Mary Hornev [redacted] <[redacted]> on behalf of Trenkle, Tony (CMS/OIS)

To: Park, Todd <[redacted]>
> Fryer, Teresa M. (CMS/OIS)
> Schankweiler, Thomas W. (CMS/OIS)
> Baitman, Frank (OS/ASA/OCIO)
> Charest, Kevin (OS/ASA/OCIO/OIS)

Cc: Mellor, Michael (CMS/OIS) <[redacted]>
> Callaghan, Liz M. (OS/ASA/OCIO)
> Byczkowski, Roxanne (CMS/OIS)
> Mielke, Dawn M.
> Velasco, Linda J. (CMS/OIS) <[redacted]>

Bcc:
Subject: Marketplace Security - NEW DAY & TIME - WebEx: [redacted] (internal); [redacted]
(external); Mtg. No. [redacted]
Date: Tue Sep 03 2013 08:40:36 EDT
Attachments:

The above-subject meeting was requested by Tony Trenkle to occur on this day at this time. If you are unable to attend this meeting, please call the OIS Front Office at [redacted].

Meeting Number: [redacted]
Meeting Password: This meeting does not require a password.

Audio conference information

1. Please call the following number:
WebEx: [redacted]
2. Follow the instructions you hear on the phone.
Your WebEx Meeting Number: [redacted]

To join from the Baltimore, Chicago, or Kansas City offices

1. Dial ext. [redacted]
2. Enter the Meeting Number: [redacted]

To start the online meeting

1. Go to [redacted]
2. If you are not logged in, log in to your account.

- Like all publicly facing Internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state of the art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff. When the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.
- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.
- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US-CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 02:43 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid' <[REDACTED]>

'Michelle.Snyder' <[REDACTED]>; 'tony.frehle' <[REDACTED]>

<[REDACTED]>; Frank.Baltman <[REDACTED]>; Graubard, Vivian

Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 2:19 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian

Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people -- they are tracking folks down today and will seek to get you additional info by tonight.... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
Todd

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 12:28 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian

Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [redacted] We need to have all of this locked down for September 11th hearing, we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 12:02 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian

Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for [redacted] The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about

next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

-- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Tuesday, September 03, 2013 7:22 PM
To: Park, Todd; Baitman, Frank (OS/ASA/OClO); Snyder, Michelle (CMS/OA)
Subject: Re: Cybersecurity points

I don't see any problem with him joining if it helps with context etc.

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, September 03, 2013 07:06 PM
To: Trenkle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OClO); Snyder, Michelle (CMS/OA)
Subject: Fw: Cybersecurity points

Tony, Frank, Michelle, thoughts on Ed joining our 10 am call tomorrow, and then talking with him afterwards briefly? One point to discuss with him is Frank's very good point that we need to walk a fine line publicly -- showing we take the risks seriously but also not baiting hackers into attacking.

Also: it was part of the outline for tomorrow's call, but just wanted to follow up on if we can get some external validators to be references with respect to CMS's general cyberdefenses and approach to cybersecurity -- again, in the context of the walking the fine line above....

Thanks so much,
Todd

----- Original Message -----

From: Siskel, Edward
Sent: Tuesday, September 03, 2013 05:14 PM
To: Park, Todd
Subject: FW: Cybersecurity points

[REDACTED]

-----Original Message-----

From: Jennings, Christopher
Sent: Tuesday, September 03, 2013 4:33 PM
To: Siskel, Edward; McGuinness, Tara; Lambrew, Jeanne; Park, Todd
Cc: Jones, Isabel; [REDACTED]; [REDACTED]; [REDACTED]; Graubard, Vivian
Subject: Re: Cybersecurity points

Todd and gang:

[REDACTED]

[Redacted]
Thanks all.

Chris

----- Original Message -----

From: Jennings, Christopher

Sent: Tuesday, September 03, 2013 07:12 AM

To: Park, Todd; Siskel, Edward

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid' <[Redacted]>;

'Michelle.Snyder' <[Redacted]>; 'frank.baitman' <[Redacted]>; 'tony.trenkle' <[Redacted]>;

<[Redacted]>; 'frank.baitman' <[Redacted]>; Graubard, Vivian

Subject: Re: Cybersecurity points

Thank you Todd and all on this email. Very helpful and greatly appreciated. [Redacted]
[Redacted] Thanks to all for this background and, more importantly, your great work to protect us from cyber attacks/security threats.

Chris

----- Original Message -----

From: Park, Todd

Sent: Tuesday, September 03, 2013 01:38 AM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid' <[Redacted]>;

'Michelle.Snyder' <[Redacted]>; 'frank.baitman' <[Redacted]>; 'tony.trenkle' <[Redacted]>;

<[Redacted]>; 'frank.baitman' <[Redacted]>; Graubard, Vivian

Subject: Re: Cybersecurity points

Hi Chris, here are an expanded/updated set of bullet points from Frank and Tony:

- Like all publicly facing Internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state-of-the-art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff. When the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.
- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.
- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US -CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 02:43 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; Aryana, Khalid <[REDACTED]>; Michelle.Snyder <[REDACTED]>; tony.trenkle <[REDACTED]>; <[REDACTED]>; frank.baitman <[REDACTED]>; Graubard, Vivian

Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

----- Original Message -----

From: Park, Todd

Sent: Monday, September 02, 2013 2:19 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; Aryana, Khalid <[REDACTED]>; Michelle.Snyder <[REDACTED]>; tony.trenkle <[REDACTED]>; frank.baitman <[REDACTED]>; Graubard, Vivian

Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people — they are tracking folks down today and will seek to get you additional info by tonight.... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
Todd

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 12:28 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'frank.baitman [REDACTED]'; 'tony.trenkle [REDACTED]'; 'Graubard, Vivian

Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [REDACTED]. We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 12:02 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid [REDACTED]'; 'Michelle.Snyder [REDACTED]'; 'tony.trenkle [REDACTED]'; 'frank.baitman [REDACTED]'; 'Graubard, Vivian

Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for you [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday — am looping Tony (CMS CO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

— The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

— CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

--- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts. --- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Tuesday, September 03, 2013 7:24 PM
To: Trenkle, Tony (CMS/OIS); Park, Todd; Baitman, Frank (OS/ASA/OCIO)
Subject: Re: Cybersecurity points

Agree with tony

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Trenkle, Tony (CMS/OIS)
Sent: Tuesday, September 03, 2013 07:22 PM
To: 'Todd_Y_Park' <[REDACTED]>; Baitman, Frank (OS/ASA/OCIO); Snyder, Michelle (CMS/OA)
Subject: Re: Cybersecurity points

I don't see any problem with him joining if it helps with context etc.

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, September 03, 2013 07:06 PM
To: Trenkle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OCIO); Snyder, Michelle (CMS/OA)
Subject: Fw: Cybersecurity points

Tony, Frank, Michelle, thoughts on Ed joining our 10 am call tomorrow, and then talking with him afterwards briefly? One point to discuss with him is Frank's very good point that we need to walk a fine line publicly -- showing we take the risks seriously but also not baiting hackers into attacking.

Also: it was part of the outline for tomorrow's call, but just wanted to follow up on if we can get some external validators to be references with respect to CMS's general cyberdefenses and approach to cybersecurity -- again, in the context of the walking the fine line above....

Thanks so much,
Todd

----- Original Message -----

From: Siskel, Edward
Sent: Tuesday, September 03, 2013 05:14 PM
To: Park, Todd
Subject: FW: Cybersecurity points

[REDACTED]

-----Original Message-----

From: Jennings, Christopher
Sent: Tuesday, September 03, 2013 4:33 PM
To: Siskel, Edward; McGuinness, Tara; Lambrew, Jeanne; Park, Todd
Cc: Jones, Isabel; [REDACTED]; Graubard, Vivian
Subject: Re: Cybersecurity points

Todd and gang:

[REDACTED]

Thanks all.

Chris

----- Original Message -----

From: Jennings, Christopher
Sent: Tuesday, September 03, 2013 07:12 AM
To: Park, Todd; Siskel, Edward
Cc: Lambrew, Jeanne; Jones, Isabel; 'aryana.khalid' [REDACTED];
'Michelle.Snyder' [REDACTED]; 'frank.baitman' [REDACTED]; 'tony.trenkle' [REDACTED];
'frank.baitman' [REDACTED]; 'tony.trenkle' [REDACTED]; Graubard, Vivian
Subject: Re: Cybersecurity points

Thank you Todd and all on this email. Very helpful and greatly appreciated. [REDACTED]
[REDACTED] Thanks to all for this background and, more importantly, your great work to protect us from cyber attacks/security threats.

Chris

----- Original Message -----

From: Park, Todd
Sent: Tuesday, September 03, 2013 01:38 AM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'aryana.khalid' [REDACTED];
'Michelle.Snyder' [REDACTED]; 'frank.baitman' [REDACTED]; 'tony.trenkle' [REDACTED];
'frank.baitman' [REDACTED]; 'tony.trenkle' [REDACTED]; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris, here are an expanded/updated set of bullet points from Frank and Tony:

- Like all publicly facing Internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state of the art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff. When the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.
- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.
- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US-CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 02:43 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; Aryana.Khalid <>

Michelle.Snyder <>; tony.trenkle <>

<>; frank.baitman <>; Graubard, Vivian

Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 2:19 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian

Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people — they are tracking folks down today and will seek to get you additional info by tonight.... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,

Todd

-----Original Message-----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 12:28 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian

Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder for [redacted] We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd

Sent: Monday, September 02, 2013 12:02 PM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid'; 'Michelle.Snyder'; 'tony.trenkle'; 'frank.baitman'; Graubard, Vivian

Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for you [redacted] The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about

next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday — am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

— The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

— CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

— The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

— Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

— As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts — we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Wednesday, September 04, 2013 8:12 AM
To: Siskel, Edward; Horney, Mary P. (CMS/OIS)
Cc: Graubard, Vivian; Mielke, Dawn M.; Park, Todd
Subject: 10 call

Mary,

Please add Ed to the appointment.

Thanks.

-----Original Message-----

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, September 03, 2013 7:53 PM
To: Siskel, Edward
Cc: Trenkle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OCIO); Snyder, Michelle (CMS/OA); Graubard, Vivian; Mielke, Dawn M.
Subject: Re: Cybersecurity points

Ed, it would be great for you to join the 10 am call hosted by Tony Trenkle tomorrow, and for a subset of us to chat with you for a few minutes after the call. Tony, can you make sure Ed gets the invite/call-in number?

Ed, it may also make sense for you to join the 4 pm mtg -- let's discuss tomorrow, thanks!

Todd

Exhibit 14

From: Jennings, Christopher
Sent: Tuesday, September 17, 2013 10:56 PM
To: Park, Todd
Subject: Fw: Final Version of PR
Attachments: FINAL Marketplace Fraud Press Release WHCO edits clean.docx; FINAL Marketplace Fraud Press Release WHCO edits.docx

From: Jones, Isabel
Sent: Tuesday, September 17, 2013 09:00 PM
To: 'Salcido, Dori (HHS/ASPA)' <[REDACTED]>; Sye, Tait (OS/ASPA) <[REDACTED]>; Jennings, Christopher; Jackson, Veronica (HHS/ASPA) <[REDACTED]>
Subject: RE: Final Version of PR

Sorry, two tiny edits attached that WHCO just told me are mistakes to keep FTC on board. I think we can go with this as final.

From: Salcido, Dori (HHS/ASPA) [mailto:[REDACTED]]
Sent: Tuesday, September 17, 2013 8:59 PM
To: Jones, Isabel; Sye, Tait (OS/ASPA); Jennings, Christopher; Jackson, Veronica (HHS/ASPA)
Subject: RE: Final Version of PR

Yes, minor tweak, but final is also attached.

Dori Salcido

[REDACTED] (o)
 [REDACTED] (c)

From: Jones, Isabel [mailto:[REDACTED]]
Sent: Tuesday, September 17, 2013 8:52 PM
To: Salcido, Dori (HHS/ASPA); Sye, Tait (OS/ASPA); Jennings, Christopher; Jackson, Veronica (HHS/ASPA)
Subject: Final Version of PR

Hi -- Attached are just last edits to incorporate changes we received from WHCO. These are very minor so we are hoping to consider these locked. Attached is tracked and clean copy. Can you let us know if we can consider this final and send us back the final version with any last minor edits fixed (any typos/formatting, etc)?

Thanks all,
 Isabel

Obama Administration announces a coordinated effort to prevent and detect consumer fraud in the Health Insurance Marketplace

Today, Attorney General Eric Holder, Health and Human Services Secretary Kathleen Sebelius, and Federal Trade Commission Chairwoman Edith Ramirez met at the White House to kick off a comprehensive interagency initiative to prevent, protect against, and where necessary prosecute consumer fraud and privacy violations in the Health Insurance Marketplaces. Representing key state partners in this critically important effort to protect consumers were Maryland Attorney General Douglas Gansler and Kansas Insurance Commissioner Sandy Praeger. Senior White House officials also attended the meeting.

Meeting participants reaffirmed their ongoing commitment to protect consumers from threats in this area. Building on a successful infrastructure that already exists, the interagency officials highlighted the following new initiatives: 1) the dedication of the Marketplace Call Center as a resource and referral to FTC for consumer fraud concerns; 2) training for the Marketplace Call Center staff to effectively refer consumer threats and complaints; 3) connecting consumers to FTC's Complaint Assistant through Healthcare.gov; 4) development of a system of routing complaints through the FTC's Consumer Sentinel Network for analysis and referral as appropriate; 5) establishment of a rapid response mechanism for addressing privacy or cybersecurity threats and; 6) release of new educational materials to empower consumers and assisters who help potential enrollees to avoid scams.

"Today we are sending a clear message that we will not tolerate anyone seeking to defraud consumers in the Health Insurance Marketplace," said Health and Human Services Secretary Sebelius. "We have strong security safeguards in the Marketplace to protect people's personal information against fraud and we will work with our partners to aggressively prosecute bad actors, just as we have been doing in Medicare, Medicaid and the Children's Health Insurance Program."

The experienced and dedicated professionals at HHS, DOJ and FTC, together with their state and local partners, are ready to anticipate and respond to the law enforcement challenges that may arise with the launch of the Marketplace. They will be using tried and tested methods for combatting fraud associated with other government programs, so that consumers can confidently and securely shop for affordable health insurance beginning on October 1.

"I am proud of the proactive approach that the Justice Department is taking with our colleagues at HHS and FTC, and with the state law enforcement community, to prevent and detect consumer fraud in the Health Insurance Marketplace," said Attorney General Eric Holder. "Going forward, we intend to share information, work cases, and hold wrongdoers accountable as we always do. We plan to use our tried-and-tested collaborative methods to ensure that we can identify trends and take swift action against those seeking to take advantage of the newly insured."

Consumers who report that their personal information may have been compromised will be given information about steps to take to prevent or respond to identity theft. If a consumer reports suspected fraud, his or her complaint will be entered into the FTC's Consumer Sentinel Network database, which is used by federal and state law enforcement agencies to track potential fraud activity. Federal law enforcement officials will be able to monitor complaint activity for trends within and across all 50 States.

"At the FTC, we know all too well how scammers invariably try to take advantage of developments in the marketplace and new government programs," said FTC Chairwoman Edith Ramirez. "We will be vigilant as always in cracking down on this type of opportunistic fraud."

Consumer fraud experts from across state and federal agencies will continue to meet on a regular basis to monitor potential fraud associated with the Marketplace and ensure the strength of preventive measures. Steps have already been initiated to prevent and respond to individuals attempting to take advantage of the public during health care implementation.

These measures include:

- **Reporting fraud mechanism:** A new feature of the Marketplace Call Center (1-800-318-2596, TTY 1-855-889-4325), will now enable individuals to report fraud simply by calling the 1800 number.
- **Training:** Call Center operators trained to take a fraud complaint, and refer them to FTC's Consumer Sentinel Network.
- **Creating new pathways:** Healthcare.gov offers easy access to connect consumers to FTC's Complaint Assistant through Health Care.Gov.
- **Establishing a routing system for complaints through a centralized database:** Routing complaints through the Sentinel Network will ensure Federal, state and local law enforcement have access to consumer complaints and can analyze and refer those complaints as appropriate.
- **Protecting personal data:** Building on last week's certification of the data hub and Health Insurance Marketplace as in compliance with the stringent security, privacy and data flow standards developed by the National Institute of Standards and Technology - the gold standard for information and independent security controls assessment - the interagency officials have also established a rapid response mechanism that will be employed in the unlikely event of a data security breach.
- **Empowering consumers with information:** Building on a proactive effort to inform consumers about potential fraud and privacy threats, the federal government is releasing new educational materials to empower consumers and assisters who are helping consumers navigate the Marketplaces. They include online tip sheets like: Protect Yourself from Fraud in the Health Insurance Marketplace [LINK <http://marketplace.cms.gov/getofficialresources/publications-and-articles/protect-yourself-from-fraud-in-health-insurance-marketplace.pdf>] and Tips for Assisters to Help Consumers Navigate the Marketplace [INSERT LINK]. The materials remind consumers that there is free assistance available to navigate the Marketplace and that they should be suspicious of persons who ask for a fee before providing assistance.

In addition, the FTC and DOJ are hosting events this week in anticipation of the launch of the Marketplace:

- Thursday, September 19th, the FTC, will host a roundtable in Washington, DC to discuss how to empower and protect consumers from scammers with the advent of the Health Insurance

Marketplace. The roundtable will bring together experts on the health care law, federal and state consumer protection officials, representatives of legal services and community-based organizations, and consumer advocates to discuss key features of the law, state approaches to implementation, and how to help consumers avoid potential scams.

- Friday, September 20th, DOJ will host a law enforcement meeting to convene state and local officials. This meeting is part of ongoing efforts urging state AGs to work with HHS and federal, state, and local law enforcement to mount a substantial outreach campaign to educate consumers about how to prevent scams and fraud and protect their personal information in the Marketplace.

These comprehensive preventive and detection efforts build on the extensive experience and federal, state and local intergovernmental infrastructure that has protected consumers from fraud.

- Since its creation in 1997, the HHS Senior Medicare Patrol has educated to more than 28 million Medicare beneficiaries and counseled more than 1.3 million individuals about specific concerns, one-on-one. Coupled with other outreach efforts, Medicare's toll-free customer service operations sent nearly 45,000 inquiries to law enforcement partners for fraud investigations in 2012 alone. These direct-from-consumer leads ultimately supported the Administration's work to prosecute criminals, returning \$6.7 billion to the Medicare Trust Fund in the last four years.
- In the last several years, the FTC's Bureau of Consumer Protection has put a stop to over 50 health fraud scams, government grant schemes, and mortgage relief services frauds, and has independently secured nearly \$6 million in monetary relief for consumers. The Bureau conducts investigations, sues companies and people that violate the law, and works to educate consumers and businesses about their rights and responsibilities. The Bureau coordinates its work in these areas with Federal, state and local partners.
- Over the last four years, DOJ has successfully prosecuted over four thousand defendants in identity theft and aggravated identity theft cases, and convicted over 200 defendants in advance fee fraud cases, over 500 defendants in consumer fraud cases, and over 100 defendants in telemarketing fraud cases.

For more information on CMS's efforts to protect consumers in the Marketplace, please visit: [Securing the Health Insurance Marketplace Fact Sheet \[INSERT LINK\]](#)

###

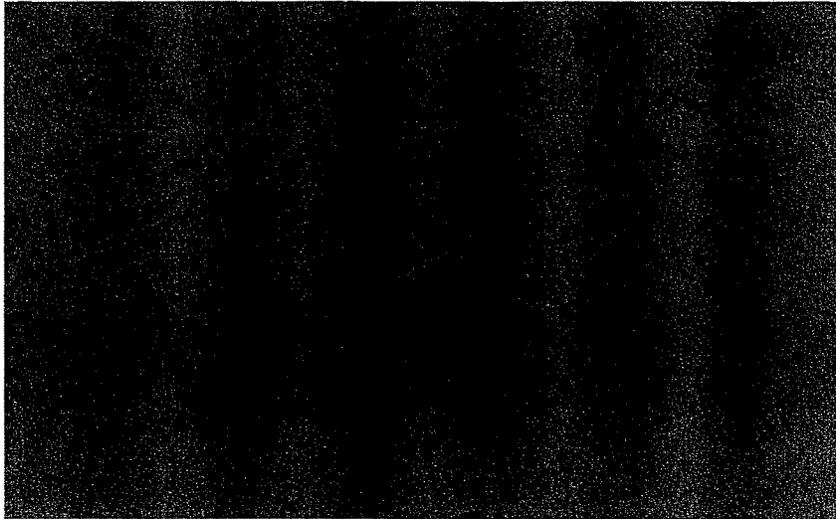
From: Park, Todd
Sent: Tuesday, September 17, 2013 4:43 PM
To: Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Trenkle, Tony (CMS/OIS); [REDACTED] Cook, Brian T. (CMS/OC) ([REDACTED])
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Jessica, I am signed up to help with the call. Looping Tony, Frank, and Brian. Two questions:

1. Is the call on background, or on the record?
2. Can Tony Trenkle and Frank Baitman join me on the call? They are the folks who know the details, and it would be super-helpful for them to be on.

Thanks!
Todd

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 2:10 PM
To: Park, Todd
Cc: Jones, Isabel; Mielke, Dawn M.
Subject: Preventing Fraud in Marketplaces - WH background call with media tomorrow?



From: Baitman, Frank (OS/ASA/OCIO) <[REDACTED]>
Sent: Wednesday, September 18, 2013 12:31 PM
To: Trenkle, Tony (CMS/OIS); Park, Todd
Subject: Re: Cyber bullet points for your review; plus a question

Just to add to Tony's earlier point: there will be only ONE ATO for the FFM. The many components together make a system that will be tested and validated end-to-end.

- Frank

From: <Trenkle, "Tony (CMS/OIS)" <[REDACTED]>
Date: Wednesday, September 18, 2013 12:13 PM
To: "Todd Y. Park" <[REDACTED]>, Frank Baitman <[REDACTED]>
Subject: Re: Cyber bullet points for your review; plus a question

Todd

Yes, that is basically it:

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, September 18, 2013 10:56 AM
To: Trenkle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber bullet points for your review; plus a question

And Tony and Frank, sorry, one more background question: the press release today says: "Together with our interagency partners, CMS has developed a rapid response mechanism to respond to a potential data breach and mitigate the effects of attempts to jeopardize the integrity of the Hub and the databases it connects."

Is this the same thing as the Incident Response capability discussed in Marilyn's letter, but with souped up interagency coordination?

Or is it something different?

Just want to make sure I represent this properly, thanks!

From: Park, Todd
Sent: Wednesday, September 18, 2013 10:32 AM
To: Trenkle, Tony (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

And Tony, one more background question: is it the case that the security testing is done by an independent contractor managed by CMS info security staff, and that the review of results, assessment, and signoff happen via you, the CISO, and CMS info security staff? Thanks!

From: Park, Todd
Sent: Wednesday, September 18, 2013 10:15 AM
To: Trenkle, Tony (CMS/OIS); Santillo, Jessica; Baitman, Frank (OS/ASA/OCIO)

From: Park, Todd
Sent: Wednesday, September 18, 2013 12:43 PM
To: 'tony.trinkle'; [REDACTED]
Subject: Re: Cyber bullet points for your review, plus a question

Thanks so much, Tony!

From: Trinkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, September 18, 2013 12:38 PM
To: Park, Todd
Subject: RE: Cyber bullet points for your review; plus a question

Todd,

Sorry, I missed this one. Yes, you are correct about the process.

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, September 18, 2013 10:32 AM
To: Trinkle, Tony (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

And Tony, one more background question: is it the case that the security testing is done by an independent contractor managed by CMS info security staff, and that the review of results, assessment, and signoff happen via you, the CISO, and CMS info security staff? Thanks!

From: Park, Todd
Sent: Wednesday, September 18, 2013 10:15 AM
To: Trinkle, Tony (CMS/OIS); Santillo, Jessica; Baitman, Frank (OS/ASA/OCIO)
Cc: Jones, Isabel; Mielke, Dawn M.; Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA); Graubard, Vivian; Vahey, Moira; Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

OK, great, Tony, thanks! Any other points you think I should have as background material?

From: Trinkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, September 18, 2013 8:30 AM
To: Park, Todd; Santillo, Jessica; Baitman, Frank (OS/ASA/OCIO)
Cc: Jones, Isabel; Mielke, Dawn M.; Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA); Graubard, Vivian; Vahey, Moira; Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

Todd,

The bullets you have written are consistent with the letter as well as the call and statement from Gartner. In terms of other ATOs, I would not characterize it that way because it sounds like we are doing a piecemeal approach. In reality

there will only be one ATO issued for the FFM, even though there are multiple components that are being tested. Here is how I would re-write the sentence:

--- CMS is working to ensure that all security testing for the Marketplace systems are completed and the appropriate operating authorities are signed before October 1.

I'm putting it in that context because the privacy and security framework for the Marketplace also includes interconnection agreements with other Federal agencies and states, agreements with issuers, and security agreements/contract language for the Marketplace contractors.

Tony

From: Park, Todd [mailto:]
Sent: Wednesday, September 18, 2013 1:18 AM
To: Santillo, Jessica; Trankle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OCIO)
Cc: Jones, Isabel; Mielke, Dawn M.; Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA); Graubard, Vivian; Vahey, Moira
Subject: Cyber bullet points for your review; plus a question
Importance: High

Hi Tony, Frank, and Jessica, please see draft cyber talking points below they are drawn from Marilyn's letter plus earlier talking points that Frank and Tony put together plus a statement that Gartner analyst Christian Barnes recently gave us about the statements in Marilyn's letter. Please let me know what you think, and made edits/additions as you see fit. I have attached the bullet points in a Word document for easier track changes editing if desired. Tony, please also note the question about additional ATOs highlighted in yellow below. Thanks!

-- We take extremely seriously our responsibility to protect personal information in the Affordable Care Act Marketplace. Collectively, the tools, methods, policies, and procedures HHS has developed provide a safe and sound security framework to safeguard consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage starting on October 1. This framework is consistent with the framework that exists for all other HHS programs, such as Medicare, on which Americans rely every day.

-- HHS's Centers for Medicare and Medicaid Services (CMS) has a strong track record of preventing breaches involving the loss of personally identifiable information from cyber-attacks. This is due in large part to the establishment of an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The system and security controls established and implemented by CMS meet tough existing Federal standards.

-- The Marketplace is designed to comply with the comprehensive information security standards developed by the National Institute for Standards and Technology (NIST) in support of the Federal Information Security Management Act (FISMA). NIST has emerged as the gold standard for information security standards and guidelines that all Federal agencies follow. Several layers of protection will be in place to help protect against potential damage from attackers and mitigate risks. For example, the Marketplace will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action against irregular behavior and unauthorized system changes that could indicate potential attacks. Automated methods will ensure that system administrators have access to only the parts of the system that are necessary to perform their jobs. These protocols, combined with continuous monitoring, will alert system security personnel when any system administrator attempts to perform functions or access data for which they are not authorized or are inconsistent with their job functions.

-- Should security incidents occur, CMS would activate an Incident Response capability built on the model developed by NIST. The Incident Response function allows for the tracking, investigation, and reporting of incidents so that HHS may quickly identify security incidents and ensure that the relevant law enforcement authorities, such as the HHS Office of Inspector General Cyber Crimes Unit, are notified for purposes of possible criminal investigation.

-- CMS's information security staff have been working closely with Marketplace IT development teams to help ensure that all required security testing is completed. Before Marketplace systems are allowed to operate and begin serving consumers, they must comply with the rigorous standards we apply to all Federal operational systems, and CMS's Chief Information Officer must authorize the systems to begin operation by issuing an Authority to Operate (ATO).

-- The Data Hub, a key routing tool that helps both the Federally Facilitated Marketplace and State-Based Marketplaces provide accurate and timely eligibility determinations (by verifying information in Federal and state databases), successfully completed its independent security testing and was authorized to operate on September 6. The completion of this testing confirms that the Hub comports with the tough standards discussed above and that CMS has implemented the appropriate procedures and safeguards necessary for the Hub to operate securely on October 1.

... CMS is working to ensure that all security testing is completed and ATO's issued for other Marketplace components as well before October 1. [QUESTION FOR TONY: have any additional ATOs been issued beyond the Hub ATO? Will there be just one additional ATO, or multiple? Is this sentence worded correctly?]

-- HHS has produced a strong enterprise information security program by implementing state-of-the-art controls and business processes based on statutory requirements, agency and organizational commitments, best practices, and the experience and knowledge of our subject matter team members.

-- As recently noted by Christian Barnes, a leader of the information security practice at Gartner Research, which advises thousands of private-sector and government clients on best practices associated with the use of information technology, this HHS/CMS information security program as described above represents "current best practices for the protection of sensitive and regulated data and systems."

-- Application of this information security program to the Marketplace provides strong, sound safeguards for consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage.

From: Park, Todd

Sent: Tuesday, September 17, 2013 9:54 PM

To: Santillo, Jessica; tony.trenkle

Cc: Jones, Isabel; Mielke, Dawn M.; frank.bajltman; Brian.Cook; Michelle.Snyder

Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Tony/Frank, an update -- it looks like the background call tomorrow is with WH folks only, with detailed inquiries to be referred to agencies.

So: while I'd love for you to hold the time on your calendars (just in case), as of this moment, you don't have to get on the call :)

I've let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can't talk to it at a general level only -- she thinks that will be OK on the call tomorrow, with detailed questions to be referred to agencies.

Just to triple check this, I will be sending around talking points tonight which (combined with Marilyn's Hub letter) basically represent what I'm prepared to say tomorrow. Would very much appreciate your vetting of these.

And in the event that, after reviewing my talking points, Jessica feels like we need more on the call, we may ask you to attend the call after all :)

So while you are off the hook for now, please do hold the call time, just in case!

Thanks so much, and please stay tuned for talking points to vet, coming later tonight,

Todd

From: Park, Todd
Sent: Tuesday, September 17, 2013 07:39 PM
To: Santillo, Jessica; 'tony.trenkle [REDACTED]' <[REDACTED]>
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman [REDACTED]' <[REDACTED]>; 'Brian.Cook [REDACTED]' <[REDACTED]>; 'Michelle.Snyder [REDACTED]' <[REDACTED]>
Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

OK, will draft talking points and send around later tonight. And Tony/Frank, please confirm if you can join me on this background call -- again, only to participate in the cybersecurity portion :) Would really appreciate your help :)

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 07:37 PM
To: Park, Todd; 'tony.trenkle [REDACTED]' <[REDACTED]>
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman [REDACTED]' <[REDACTED]>; 'Brian.Cook [REDACTED]' <[REDACTED]>; 'Michelle.Snyder [REDACTED]' <[REDACTED]>
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Thanks Todd if your team could draft the cyber talking points, that would be very helpful. Thanks so much.

We are still working on finalizing the paper but will share those with everyone as soon as they are ready.

From: Park, Todd
Sent: Tuesday, September 17, 2013 7:22 PM
To: Santillo, Jessica; 'tony.trenkle [REDACTED]' <[REDACTED]>
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman [REDACTED]' <[REDACTED]>; 'Brian.Cook [REDACTED]' <[REDACTED]>; 'Michelle.Snyder [REDACTED]' <[REDACTED]>
Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Thanks, Jessica, Tony and Frank, can you join via phone? You'll only be asked to help with the cybersecurity part of the call :) I am more than happy to deliver the primary talking points, which will focus principally on Marilyn's letter regarding Hub cybersecurity + the general points the three of us hammered out a while back.

Jessica, are you putting together talking points for us, or would you like me to take a crack at them?

Thanks,
Todd

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 07:13 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS) <[REDACTED]>
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO) <[REDACTED]>; Cook, Brian T. (CMS/OC) <[REDACTED]>; Snyder, Michelle (CMS/OA) <[REDACTED]>
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Todd happy to have Tony and Frank join us for the cyber security portion.

On your first question the call is on background according to "White House officials."

Thanks very much for making this work on such short notice. We will hold the call in EEOB 207. I will send around a calendar invite.

Thank you again,
Jessica

From: Park, Todd
Sent: Tuesday, September 17, 2013 6:14 PM
To: Trenkle, Tony (CMS/OIS); Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Tony, the part of the call where you, Frank, and I would be participating would focus exclusively on cybersecurity....
Jessica, thoughts?

From: Trenkle, Tony (CMS/OIS) [mailto:]
Sent: Tuesday, September 17, 2013 5:08 PM
To: Park, Todd; Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Todd,
I am not really comfortable about participating on this call, even on background. It is getting into areas that I have not been involved in (privacy and fraud prevention efforts).
Tony

From: Park, Todd [mailto:]
Sent: Tuesday, September 17, 2013 4:43 PM
To: Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Trenkle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Jessica, I am signed up to help with the call! Looping Tony, Frank, and Brian. Two questions:

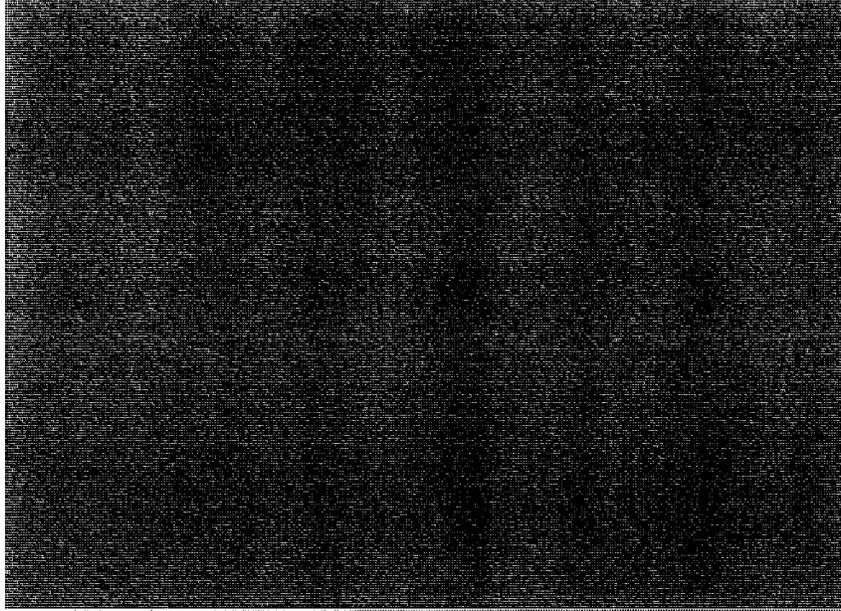
1. Is the call on background, or on the record?
2. Can Tony Trenkle and Frank Baitman join me on the call? They are the folks who know the details, and it would be super-helpful for them to be on.

Thanks!
Todd

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 2:10 PM

400

To: Park, Todd
Cc: Jones, Isabel; Mielke, Dawn M.
Subject: Preventing Fraud in Marketplaces - WH background call with media tomorrow?



From: Trenkle, Tony (CMS/OIS) <[REDACTED]>
Sent: Wednesday, September 18, 2013 4:25 PM
To: Park, Todd; Santillo, Jessica; Baitman, Frank (OS/ASA/OCTO)
Cc: Jones, Isabel; Mielke, Dawn M.; Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA); Graubard, Vivian; Vahey, Moira; Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

Todd,

Glad to help and I had no doubt that you could deftly handle all of the questions. You probably now have at least a Bachelors' degree in CMS. I will let Gartner know.

tony

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, September 18, 2013 2:09 PM
To: Trenkle, Tony (CMS/OIS); Santillo, Jessica; Baitman, Frank (OS/ASA/OCTO)
Cc: Jones, Isabel; Mielke, Dawn M.; Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA); Graubard, Vivian; Vahey, Moira; Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

Hi all, the background call went well (knock on wood will wait to see the coverage). Thank you all very much Tony, Team CMS and Frank especially for all of your help! On cyber, I basically delivered a condensed version of the talking points below.

Tony, I did indeed cite Gartner's statement as referenced in the bullet points below, and referenced Christian's name specifically you may want to give Gartner/Christian a heads up about that.

The only question we got on cyber was a question about the Hub ATO on Sept 6 and whether security testing for the Marketplace was done. The answer I gave was that security testing was now complete for the Hub, which is a critical component of the overall Marketplace. Security testing continues for other components of the Marketplace, and CMS is working to ensure that all security testing for Marketplace systems is completed and associated authority to operate is issued before October 1.

Jessica, please let us know if you get any follow-up questions thanks!

Todd

From: Trenkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, September 18, 2013 8:30 AM
To: Park, Todd; Santillo, Jessica; Baitman, Frank (OS/ASA/OCTO)
Cc: Jones, Isabel; Mielke, Dawn M.; Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA); Graubard, Vivian; Vahey, Moira; Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Cyber bullet points for your review; plus a question

Todd,

The bullets you have written are consistent with the letter as well as the call and statement from Gartner. In terms of other ATOs, I would not characterize it that way because it sounds like we are doing a piecemeal approach. In reality

Exhibit 15

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
 Sent: Sunday, September 29, 2013 4:00 PM
 To: Chao, Henry (CMS/OIS); Park, Todd
 Subject: Re: Food tomorrow

I am such an ogre!! Of course - eat a cupcake for me

M

Sent from my BlackBerry Wireless Device

From: Chao, Henry (CMS/OIS)
 Sent: Sunday, September 29, 2013 02:41 PM
 To: Park, Todd <[REDACTED]>
 Cc: Snyder, Michelle (CMS/OA)
 Subject: RE: Food tomorrow

I think you can come in and help dole out the food and say hello. People here want to be able to at least see you in person. It really makes them feel like someone cares enough about their contribution to do this kind of thing so come in for at least 30 minutes but don't wander to where the architects and engineers (the ones you took a picture with) are because they will never let you leave.

Michelle is it ok for him to come in for 30 minutes and help serve?

Henry Chao
 Deputy CIO & Deputy Director,
 Office of Information Services
 Centers for Medicare & Medicaid Services
 [REDACTED]

From: Park, Todd (mailto:[REDACTED])
 Sent: Sunday, September 29, 2013 2:38 PM
 To: Chao, Henry (CMS/OIS)
 Cc: Snyder, Michelle (CMS/OA)
 Subject: Re: Food tomorrow

I have the cupcakes -- to manage expectations, they did not have 150 red velvet in stock, so I had to supplement with other flavors :) I will subsequently acquire ice cream. Will hit the road after the 5 pm call -- so would estimate an ETA of 6:30-7 pm. My dad is driving me to ensure the well being of other people on the road :) And as per my promise to Michelle, I will drop off the cupcakes and ice cream and immediately leave :)

From: Park, Todd
 Sent: Sunday, September 29, 2013 01:41 PM
 To: 'henry.chao' <[REDACTED]>
 Cc: 'Michelle.Snyder' <[REDACTED]>

Subject: Re: Food tomorrow

Am on it :)

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Sunday, September 29, 2013 01:31 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA) < >
Subject: RE: Food tomorrow

Cupcakes are for anytime.

Ice cream has never been served here so that will be a surprise.

Tammy (CGI master at taking care of all the staff) has already ordered tonight's dinner so you are in charge of the out of the ordinary surprises.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Park, Todd [mailto:]
Sent: Sunday, September 29, 2013 1:29 PM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA)
Subject: Re: Food tomorrow

I can also totally bring dinner -- just let me know.... Called Georgetown Cupcake, and am going to stand in line at the store now for the cupcakes :)

From: Park, Todd
Sent: Sunday, September 29, 2013 01:24 PM
To: 'henry.chao' < >
Cc: 'Michelle.Snyder' < >
Subject: Re: Food tomorrow

Don't think I got the other email.... But to clarify, I should not bring dinner, but rather, red velvet cupcakes from Georgetown Cupcake and Haagen Daz for 150 folks -- yes? If so, I should jump on that -- the Georgetown Cupcake part in particular -- right now :)

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Sunday, September 29, 2013 01:20 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA) < >
Subject: Re: Food tomorrow

See my later email...

Red velvet cupcakes from Georgetown Cupcakes and Haagen Dazs ice cream bars for about 150 people.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244



From: Park, Todd [mailto:]
Sent: Sunday, September 29, 2013 01:18 PM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA)
Subject: Re: Food tomorrow

Hi Henry, for roughly how many folks should I get dinner? Don't spend more than 10 seconds answering, and err on the high side :)

From: Chao, Henry (CMS/OIS) [mailto:]
Sent: Saturday, September 28, 2013 11:57 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA) < >
Subject: Re: Food tomorrow

The address is 593 Herndon Plwy, Herndon VA. CGI is on the 3rd floor and you need an escort to get in on the weekend so you can call me.

There's a fantastic admin person who takes care of ordering food so I will check with her in the morning on whether if lunch or dinner is better and also get you a count.

I'll call you in the morning but I think likely I think it will be dinner.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244



From: Park, Todd [mailto:]
Sent: Saturday, September 28, 2013 11:34 PM
To: Chao, Henry (CMS/OIS)

406

Cc: Snyder, Michelle (CMS/OA)
Subject: Food tomorrow

Hi Henry, I have permission from Michelle to bring y'all food tomorrow in Herndon on the condition that I leave immediately after delivering the food and not involve you in a long and super-interesting conversation that takes time away from your incredibly important work ☺

Question #1: for how many people should I bring food? I want to bring food for everyone that is working there.

Depending on your answer, I may bring lunch or dinner - dinner if the number is really big, because it may take me some time to rustle up that much food ☺

Question #2: What is the address again of the Herndon building?

Thanks!

Todd

Exhibit 16

From: Park, Todd [mailto: [REDACTED]]
 Sent: Monday, September 30, 2013 11:43 PM
 To: Fasching, Laura; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
 Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) [REDACTED]; Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
 Subject: RE: New expansion

Laura, thanks so very, very much Henry and I will be awake, by our mobiles, and online, awaiting with bated breath what your team's ingenuity can cook up!

From: Fasching, Laura [mailto: [REDACTED]]
 Sent: Monday, September 30, 2013 11:34 PM
 To: Park, Todd; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
 Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) [REDACTED]; Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
 Subject: RE: New expansion
 Importance: High

Todd, thanks the team is looking for options to assist in speeding up the deployments & VM builds give us a little bit to see what else we can do to assist.

Thanks
 Laura

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: [REDACTED]
 222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto: [REDACTED]]
 Sent: Monday, September 30, 2013 11:02 PM
 To: Fasching, Laura; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
 Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) [REDACTED]; Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
 Subject: RE: New expansion
 Importance: High

Dear Laura, David, and Chris, thank you so very much for the heroic work you have done and are doing to support Marketplace go-live! We have one more favor to ask:

I understand from Henry that a Verizon/Terremark team is working very hard to activate all the new hardware that's arrived at Culpeper.

Every new VM, every ounce of additional power adds materially to the probability of a successful go-live tomorrow morning.

If there is any possible way that you could 2x, 3x, 4x progress by having teams work in parallel tonight, that would be absolutely amazing.

Possible?

This is a historic moment, and the team is so very close to pulling off a feat for the ages – is there any way to amp things up even further?

We would be massively, massively appreciative – please contact Henry with questions/thoughts!

All the best,
Todd

Todd Park
United States Chief Technology Officer and Assistant to the President
Executive Office of the President

Mobile: [REDACTED]

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Monday, September 30, 2013 7:22 PM
To: Chao, Henry (CMS/OIS); Park, Todd
Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR); Fasching, Laura
Subject: RE: New expansion

All, good news!

The first 2 new compute pools are being presented to InfiniCenter now, barring any issues they should be ready in about an hour.

New Compute Pool One (630):

Ghz: 1200
RAM: 2.4 TB
Storage: 40 TB

New Compute Pool Two (631):

Ghz: 1200
RAM: 2.4 TB
Storage: 40 TB

As we discussed today by putting 40TB of storage on each compute pool this leaves you with only 20 TB of Storage which we will allocate 10TB to each pool and turn them up sometime tomorrow.

To meet the new storage requirements that we were given today, which is 40TB for each new compute pool, which there will be 7 new compute pools – we are re locating/ re allocating a NetApp device to your environment. To support this new Net App device, we now have to have additional power run to the cage, as we had already utilized the power that was in place for previously planned expansions.

We anticipate that the new power builds will be completed at noon tomorrow, and we have scheduled the NetApp technicians to be at the data center at noon to configure the devices. When they have completed

their work we can present the additional storage to the second set of new compute pools. While we are working to have the compute and 10TB of storage stood up earlier in the day tomorrow we should have the full storage provision very late on 10/1 or very early on 10/2.

New Compute Pool Three (632):	New Compute Pool Four (633):
Ghz: 1200	Ghz: 1200
RAM: 2.4 TB	RAM: 2.4 TB
Storage: 10 TB (need to move 6290 to support 30TB)	Storage: 10 TB (need to move 6290 to support 30TB)

I will know more about the final set of 3 new compute pools; tomorrow afternoon.

if you need more storage than what was discussed today, please let us know as we will need to source additional devices.

Thanks
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Monday, September 30, 2013 12:06 AM
To: Park, Todd; Fasching, Laura
Cc: Um, Peter (CMS/CTR); Sharma; Hement (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
Subject: RE: New expansion

Working with Peter and Hemant to configure the Production environment to accommodate what I calculated on the back of an envelope to be about 550 Virtual Machines by morning of October 1st and taking a conservative estimate of a more complex set of processing loads through the system I think we will have more like a range between 90k to 110k concurrent users depending on the level of complexity of the processing loads.

Will get closer to real numbers as we run more tests and Terremark/URS builds the VMs and release them to us to configure.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Park, Todd [mailto:]
Sent: Sunday, September 29, 2013 11:37 PM
To: 'Fasching, Laura'; Chao, Henry (CMS/OIS)
Subject: RE: New expansion

Laura, fantastic, thank you!

Henry, quick question: if these two expansions get operationalized for go-live, how far down the path to the 130,000 concurrent users does it take us?

And Laura, when would the 3rd third get deployed?

Thanks!

From: Fasching, Laura [mailto:]
Sent: Sunday, September 29, 2013 11:32 PM
To: henry.chao; Park, Todd
Cc: Fasching, Laura
Subject: New expansion

Henry & Todd

The builds are going well thus far. We working to complete the first third of your expansion. The team is working now and we are hoping to deliver the first 2500 Ghz earlier than COB with the second third of approx. 2600Ghz later on Monday.

I will be at the XOC in Columbia tomorrow we are running 3 shifts of a PM/SM resource to coordinate and assist with questions, requests & escalations.

I will update you all on the equipment again early tomorrow.
Thanks
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Tenetmark
Tel: [redacted]
222 W. Las Colinas Blvd, Irving, Texas, 75039

From: Fasching, Laura <[REDACTED]>
 Sent: Tuesday, October 01, 2013 2:53 AM
 To: Park, Todd; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]; Fasching, Laura
 Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
 Subject: RE: New expansion

Todd & Henry,

URS has brought in more resources to assist with trouble shooting and builds.

We continue to keep the teams engaged and working toward our goal of a successful launch.

Laura

Laura Fasching
 Director of Public Sector Strategic Accounts | Verizon Terremark
 Tel: [REDACTED]
 222 W. Los Colinas Blvd., Irving, Texas, 75039

From: Fasching, Laura
 Sent: Tuesday, October 01, 2013 2:08 AM
 To: Park, Todd; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
 Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR); Fasching, Laura
 Subject: RE: New expansion

Todd & Henry

As we have been working with your team to assist you in making the Marketplace launch successful, we continue to work to adapt to your needs.

Right now, I understand that while we add more compute, the team needs the VMs built faster.

In this tasking we are using the best practices that were agreed to as to not induce risk into your builds

- such as utilizing the kickstart process (custom templates of the hardened images) for RHEL 5 & 6; Windows VMs, the SQL VMs utilizes a standard image which requires additional time to harden to NIST standards.

However we have found that due to the size of this environment 1500+ VMs, we are seeing an impact to running too many builds at once. As doing too builds at once slows down the process by overwhelming the Virtual Center server.

The options we have to increase the speed of the VM builds introduce a **SIGNIFICANT RISK** to the environment. We do not suggest either of these options, but I wanted to give you a full picture of the situation.

1. VC Client - Basically cloning of existing VMs and while this may seem an easy option
 - a. Old network configs and FW rules have to be removed first. Then the new ones need to be done. very time consuming and manual
 - b. Finally, these VMs will not appear in iCenter. Without them being visible in iCenter, these VMs will be unmanageable in the future & you will not be able to manage the compute resources.

2. VM import may get the VM's in place but they have the exact same issues as noted above.

We have engaged our vendor QRS to increase staffing during this time, and will follow up shortly on the results of that endeavor. If we can get a couple more people in now it will assist with allowing some team members to focus on the builds while other field calls and assist with troubleshooting.

Just as we did yesterday when we receive a request for more storage resources than were in either the reserve capacity or in the expansion order. We will work to adapt to your needs during as you bring the Affordable Care Act's Insurance Exchanges to the American public.

Thanks

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Monday, September 30, 2013 11:40 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
Subject: RE: New expansion

Laura, thanks so very, very much. Henry and I will be awake, by our mobiles, and online, awaiting with bated breath what your team's ingenuity can cook up!

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Monday, September 30, 2013 11:34 PM
To: Park, Todd; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR)
Subject: RE: New expansion
Importance: High

Todd, thanks the team is looking for options to assist in speeding up the deployments & VM builds. Give us a little bit to see what else we can do to assist.

Thanks

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Monday, September 30, 2013 11:02 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS);

MAJORITY STAFF REPORT SUBMITTED BY SUBCOMMITTEE CHAIRMAN PAUL BOURN

**Did the White House Knowingly Put Americans' Sensitive
Information at Risk?**

**Committee Seeks to Clarify Contradictions Surrounding Senior White House
Official's Role in Developing HealthCare.gov**



A Report by the Majority Staff of the
Science, Space, and Technology Committee
U.S. House of Representatives to
Chairman Lamar Smith, Committee on Science, Space, and Technology
and Chairman Paul Broun, Subcommittee on Oversight

October 2014

Table of Contents

Executive Summaryp.3

Introduction.....p.5

Mr. Park’s Involvement with Cybersecurity Standards & Protocols for HealthCare.gov and Providing Public Assurancesp.5

Mr. Park’s Misrepresentation Before Congress.....p.7

Mr. Park’s OSTP Employment and Role as HealthCare.gov Liaison to the White Housep.10

Conclusionp.12

Attachmentsp.14

Executive Summary

The data passing through the HealthCare.gov website is one of the largest federal collections of personal information ever assembled, linking individuals' information from multiple federal agencies along with state agencies and government contractors. In order to browse insurance plans, users must input personally identifiable information, including: contact information, home address, birth dates and social security numbers for all family members, and employer and income information. Independent security experts have warned that such information is vulnerable to hackers and cyber criminals because of inadequate testing and security built into the HealthCare.gov website.¹

While the Centers for Medicare and Medicaid Services (CMS) had the lead in the development of the Federally Facilitated Marketplace (FFM), including the HealthCare.gov website, former U.S. Chief Technology Officer (CTO) and Assistant to the President, Todd Park, appears to have been intimately involved with the development of HealthCare.gov, including its cybersecurity standards and protocols.

On November 13, 2013, Mr. Park testified under oath before the House Oversight and Government Reform Committee (OGR) that he did not **“actually have a really detailed knowledge”** of the website before it was launched and was **“not deeply familiar with the development and testing regimen that happened prior to October 1.”**²

However, a review of emails provided to the House Oversight and Government Reform Committee from the Department of Health and Human Services (HHS), which oversees CMS, indicates that:

- Mr. Park communicated regularly with all major government and contractor personnel involved with the website's development prior to October 1;
- Mr. Park appears to have been a principal liaison to the White House and the press about development of the HealthCare.gov website prior to its ill-fated launch; and
- Mr. Park appears to have been a contributing source of schedule pressure that the website be launched on October 1, 2013.

While serving as U.S. CTO and as an Assistant to the President, Mr. Park was Co-Chair of the Affordable Care Act Information Technology Exchange Steering Committee (Steering Committee). The Steering Committee met monthly during key stages of HealthCare.gov development, and was tasked with directly overseeing both security and privacy interagency working groups. In addition, the Steering Committee's charter explicitly directed its participants “to promote resolution of key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government with the state exchanges.”³

A month before the website's launch, Mr. Park emailed former CMS Chief Information Officer Tony Trenkle about convening a meeting on Marketplace security in the next week that **“would include**

¹ Jim Finkle and Alina Selyukh, “Some cyber security experts recommend shutting Obamacare site,” Reuters (November 19, 2013), available at: <http://www.reuters.com/article/2013/11/19/net-us-usa-healthcare-security-idUSBRE9A10NR20131119>.

² “Obamacare Implementation – The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, November 13, 2013, available at: <http://oversight.house.gov/hearing/obamacare-implementation-rollout-healthcare.gov>. (Emphasis added). *[There is a discrepancy between the Committee's official transcript and what Mr. Park said at the hearing. The official transcript quotes Mr. Park to say, “not even familiar with the development and testing regimen that happened prior to October 1.”]*

³ The Affordable Care Act IT Exchanges Steering Committee Charter, May 2012. [OSTP ACA 000161 – OSTP ACA 000168].

a discussion of our defenses, the threats, and our responses to the threats.”⁴ In that same email, Mr. Park asks for a memo **“that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi – for internal use only.”⁵**

It is difficult to reconcile Mr. Park’s statements under oath with the emails received thus far from HHS regarding his involvement with HealthCare.gov. The website was flagged in the weeks leading up to October 1st by CMS Chief Information Security Officer Teresa Fryer, who provided warnings “both verbally and in a briefing that disclosed ‘high risks’ and possible exposure to ‘attacks.’”⁶ Due to those concerns, Ms. Fryer recommended denial of the FFM’s authority to operate, a critical authorization needed for the system to launch on October 1, 2013.

Following the failed launch of HealthCare.gov on October 1, 2013, House Science, Space, and Technology Committee (SST or Committee) Chairman Lamar Smith requested that Mr. Park testify at a hearing on November 19, 2013 to examine security and privacy concerns in conjunction with the website. The White House declined the invitation, and subsequently refused to make him available on multiple occasions, explaining that Mr. Park would only testify if he was subpoenaed.

Instead of participating in a hearing, the White House offered to make Mr. Park available to brief Members of the Committee’s Subcommittee on Oversight, which was scheduled for September 10, 2014. However, the White House canceled the briefing less than 24 hours in advance when they were informed that the meeting would be transcribed.

Mr. Park’s refusal to testify before the Committee about his involvement with the security, development, and testing of HealthCare.gov has left the Committee with no other recourse but to authorize a subpoena to compel his appearance before the Subcommittee on Oversight on November 19, 2014. In addition, because of the number of discrepancies in Mr. Park’s testimony before Congress and Mr. Park’s emails provided by HHS, the Committee also authorized a subpoena of OSTP for any and all documents related to Todd Park’s involvement with HealthCare.gov.

⁴ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Tony Trenkle, Chief Information Officer, CMS, et al. (August 28, 2013) [HHS-0110802] (Emphasis added).

⁵ *Ibid.*

⁶ Sharyl Attkisson, “High Security Risk Found After HealthCare.gov launch,” CBS News (December 20, 2013), available at: <http://www.cbsnews.com/news/high-security-risks-found-after-healthcaregov-launch/>

I. Introduction

It appears that Todd Park was involved with cybersecurity standards and protocols for the HealthCare.gov website, despite statements to the contrary made by both him and Dr. Holdren. Mr. Park participated in background briefings for the press that included public assurances of the safety of the website prior to its launch in October 2013. Further, despite his testimony before the House Oversight and Government Reform Committee last November, Mr. Park appears to have been intimately involved with the development of the HealthCare.gov website. Finally, in contradiction to statements made by Office of Science and Technology Policy (OSTP) Director John Holdren, Mr. Park was employed by and worked for OSTP, and in that role, he appears to have been the main liaison between HHS, CMS, and the White House on HealthCare.gov development.

This report reflects the information available to the Committee thus far. It explains the need for more information from OSTP in addition to Mr. Park's testimony before the Committee, given concerns about potential obstruction of relevant information about Mr. Park's role and responsibilities in the development, testing, and security of the HealthCare.gov website.

II. Mr. Park's Involvement With Cybersecurity Standards & Protocols for HealthCare.gov and Providing Public Assurances

Congressional investigations into the flawed HealthCare.gov website have identified varying degrees of concern among government officials involved with the development of the website. A Centers for Medicare and Medicaid Services memo on the Federally Facilitated Marketplaces (FFM) System dated September 3, 2013, less than one month before going active, noted that "[t]here is the possibility that the FFM security controls are ineffective,"⁷ and that "[i]neffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise."⁸ Later that month, a memo addressed to CMS Administrator Marilyn Tavenner stated, "From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM."⁹ Further, a senior information security expert at CMS testified that she recommended against launching the HealthCare.gov website on October 1, 2013 because of "**high risk security concerns**."¹⁰

In multiple communications from OSTP staff, it has been repeatedly stated that Mr. Park had little involvement in the development of HealthCare.gov prior to October 1, 2013. Specifically:

- In a letter to the Committee (dated November 8, 2013), OSTP Director John Holdren stated:

"OSTP has not been substantially involved in the privacy and security standards that are in place for HealthCare.gov."¹¹

⁷ CMS Memo, "Authorization Decision for the Federal Facilitated Marketplaces (FFM) System," available at: http://oversight.house.gov/wp-content/uploads/2013/11/09_3_13-Trenkle.pdf

⁸ *Ibid*.

⁹ Memo to Marilyn Tavenner from James Kerr and Henry Chao, "Federally Facilitated Marketplace – DECISION," September 27, 2013, available at: <http://www.scribd.com/doc/180332001/CMS-Memo-on-Marketplace-Security>

¹⁰ House Oversight and Government Reform Committee press release, "CMS Officials Launched HealthCare.gov Against Warning of Agency's Top Cybersecurity Official," December 20, 2013, available at: <http://oversight.house.gov/release/cms-officials-launched-healthcare-gov-warning-agencys-top-cybersecurity-official>. (Emphasis added)

¹¹ OSTP letter to SST, November 8, 2013. (Emphasis added).

- Before the House Oversight and Government Reform Committee’s Hearing on November 13, 2013, Mr. Park himself stated:

“I don’t actually have a really detailed knowledge base of what actually happened pre-October 1.”¹²

“I am not deeply familiar with the development and testing regimen that happened prior to October 1. So I can’t really opine about that.”¹³

“I am part of an all-hands-on-deck effort to mobilize across the Administration to actually help under Jeff Zients’ leadership. And in the lead-up to October 1, that wasn’t part of my role.”¹⁴

- In a letter to the Committee (dated November 14, 2013), OSTP Director John Holdren stated:

“[T]he Office of Science and Technology Policy (OSTP) has not been substantially involved in the privacy and security standards for HealthCare.gov. Thus, neither Mr. Park nor any other OSTP staff member is in a position to testify on the data security standards of the website.”¹⁵

- In a letter to the Committee (dated July 3, 2014), OSTP Director Holdren said:

“Mr. Park and OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace’s (FFM) security measures. In attempting to arrive at an appropriate accommodation, this is worth emphasizing. Mr. Park is not a cybersecurity expert; he did not develop or approve the security measures in place to protect the website, and he does not manage those responsible for keeping the site safe.”¹⁶

Notwithstanding these denials, many of Mr. Park’s emails to HHS and CMS leadership in charge of the development of the HealthCare.gov website show what appears to be substantial involvement with the development of the website’s privacy and security standards. One email from August 2013 shows Mr. Park emailing Tony Trenkle, who was CMS Chief Information Officer at the time, about convening a meeting on Marketplace security in the next week that “*would include a discussion of our defenses, the threats, and our responses to the threats.*”¹⁷ Mr. Park then asks Mr. Trenkle to prepare a memo “*that basically outlines the protection strategy, including threat assessment and response strategy.*”

¹² “Obamacare Implementation – The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, November 13, 2013, available at: http://oversight.house.gov/wp-content/uploads/2014/06/11-13-13-TRANSCRIPT-Obamacare-Implementation-The-Rollout-of-HealthCare.gov_.pdf. (Emphasis added).

¹³ *Ibid.* (Emphasis added). [There is a discrepancy between the Committee’s official transcript and what Mr. Park said at the hearing. The official transcript quotes Mr. Park to say, “not even familiar with the development and testing regimen that happened prior to October 1.”]

¹⁴ *Ibid.* (Emphasis added).

¹⁵ OSTP letter to SST, November 14, 2013. (Emphasis added).

¹⁶ OSTP letter to SST, July 3, 2014. (Emphasis added).

¹⁷ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Tony Trenkle, Chief Information Officer, CMS, et.al. (August 28, 2013) [HHS-0110802] (Emphasis added).

*This will be a memo that we pass on to WH leadership as well, fyi – for internal use only.*¹⁸ Further, Mr. Park states that he will reach out to the CEO of Palantir Technologies, a computer software company that specializes in data analysis, *“Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace – we should do a confidential, cone of silence consult with him after we’ve had our meeting as per item 1, not before; I’ll set this up at the appropriate moment.”*¹⁹

Following that call on Marketplace security, during an email exchange between Mr. Trenkle and Mr. Park, Mr. Park asks, *“what is the best and most efficient way to prep and utilize MITRE as an external validator”*²⁰ and then suggests that *“on the Palantir call, my thought is to ask them to assume the role of a general cyber sounding board, ask them what they would be most worried about if they were us, and how they would think about defense/mitigation.”*²¹

In addition, Mr. Park notes that the memo he requested earlier is for internal eyes, but that it may be used for external purposes as well. Frank Baitman, Deputy Assistant Secretary for Information Technology at the Department of Health and Human Services, then jumps in on the email chain and writes, *“But, for public facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage,”* which Mr. Park concurs with in a responding email.²²

While these email exchanges occurred about one month prior to the launch of the HealthCare.gov website, Mr. Park was involved with security issues of the website much earlier in its development. Mr. Park participated in a meeting entitled, “National Strategy for Trusted Identities in Cyberspace (NSTIC)” at the White House Conference Center in August 2012 that was *“a technical briefing with CMS for an updated [sic] on their identity management work for the ACA Exchanges.”*²³ A few months later, Mr. Baitman forwarded an email with the subject line “Meeting with the National Security Staff and OMB” to Mr. Park where he wrote, *“Todd, here’s the note from Michael Daniel. Would you want to follow up with him to get more details on the objective of the meeting? Tony and I chatted about it this morning, and we’re concerned that there’ll be a push to make ACA identity proofing NSTIC compatible from the start: that’s definitely on our roadmap, but as we discussed, that needs to be v.2. In fact, that point has been made at previous WH meetings.”*²⁴

III. Mr. Park’s Misrepresentation Before Congress

On November 13, 2013, Mr. Park testified before the House Oversight and Government Reform Committee after he was subpoenaed to appear.²⁵ The following excerpts from the hearing transcript raise several questions:

¹⁸ *Ibid.* (Emphasis added).

¹⁹ *Ibid.* (Emphasis added).

²⁰ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Tony Trenkle, Chief Information Officer, CMS, et al. (September 4, 2013) [HHS-0106529] (Emphasis added).

²¹ *Ibid.* (Emphasis added).

²² Email from Frank Baitman, Deputy Assistant Secretary for Information Technology, HHS, to Todd Park, U.S. Chief Technology Officer, OSTP (August 28, 2013) [HHS-0110800] (Emphasis added).

²³ Email from Laura Lynch, OMB, to Todd Park, U.S. Chief Technology Officer, OSTP, et al. (August 21, 2012) [HHS-0106380] (Emphasis added).

²⁴ Email from Frank Baitman, Deputy Assistant Secretary for Information Technology, HHS, to Todd Park, U.S. Chief Technology Officer, OSTP (April 12, 2013) [HHS-0106600] (Emphasis added).

²⁵ “Obamacare Implementation – The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, November 13, 2013, available at http://oversight.house.gov/wp-content/uploads/2014/06/11-13-13-TRANSCRIPT-Obamacare-Implementation-The-Rollout-of-HealthCare.gov_.pdf

- **Rep. Scott DesJarlais** asked: “Okay, Mr. Park, would you, knowing what you know now, ask to have this [the HealthCare.gov website] delayed or pushed back?”

Mr. Park responded: “I don’t actually have a really detailed knowledge base of what actually happened pre-October 1. I don’t know what levers were available. So I would hesitate to make any point now.”²⁶

- In response to a question by **Rep. Trey Gowdy** regarding how much more testing of the website Mr. Park would have done prior to launching:

Mr. Park replied, “I am not deeply familiar with the development and testing regimen that happened prior to October 1. So I can’t really opine about that.”²⁷

- **Rep. Gowdy** continued this line of questioning: “If you are being asked to fix this after October 1st, in a couple of weeks, where were you for the first 184 weeks after the so-called Affordable Care Act passed? Where did they have you hidden?”

Mr. Park replied: “Sir, in my role at the White House as USCTO in the Office of Science and Technology Policy, I am a technology and innovation policy advisor. So I had a broad portfolio of responsibilities.”²⁸

Rep. Gowdy: “But you are obviously good enough that they brought you in to fix what was broken. It has been called a train wreck. That is not fair to train wrecks. It has been called other things. They brought you in to fix it. Why didn’t they bring you in to start it? Why are you doing a reclamation project? Why didn’t you build it?”

Mr. Park: “I am part of an all-hands-on-deck effort to mobilize across the Administration to actually help under Jeff Zients’ leadership. And in the lead-up to October 1, that wasn’t part of my role.”²⁹

Mr. Park’s denial of “detailed knowledge” and familiarity with the website in this hearing does not appear to be supported by many of Mr. Park’s own emails to HHS and CMS. In one email from Mr. Park to Mr. Henry Chao, CMS Deputy CIO and a key manager in the development of HealthCare.gov, sent just two days before the HealthCare.gov website was released to the public, Mr. Park asks about the performance and diagnostic testing of the whole system, how many users it can handle, and what happens following certain user number thresholds.³⁰ Specifically, Mr. Park asks:

“--Has the team run performance/diagnostic testing on the whole FFM, so that we know that the Marklogic bottleneck is in fact the critical, rate-limiting one, as opposed to another

²⁶ Ibid. (Emphasis added).

²⁷ Ibid. (Emphasis added). [There is a discrepancy between the Committee’s official transcript and what Mr. Park said at the hearing. The official transcript quotes Mr. Park to say, “not even familiar with the development and testing regimen that happened prior to October 1.”]

²⁸ Ibid. (Emphasis added).

²⁹ Ibid. (Emphasis added).

³⁰ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Henry Chao, Deputy CIO, CMS, et al (September 29, 2013) [QSSI-OGR-0000133317].

bottleneck in, say, Plan Compare or elsewhere, that could also constrain the number of concurrent users?

--In other words, does the performance testing the team is doing make you confident that the FFM across the board can indeed take 16,000 concurrent users, rising to 60,000-70,000 with the new hardware? -- So far we were able to run 2000 concurrent users in IMP1B...

--Are we going to run performance testing today and tomorrow on the growing aggregate collection of hardware (not just one unit of it), so we validate the projections of 16,000/60,000-70,000 with the actual production machinery?

--Are we testing to make sure that incoming traffic gets properly load balanced across the VM/units? (This may be accomplished by the previous item)

--What happens after the 16,000/60,000-70,000 threshold is reached? Is there gradual degradation of response time for users? Rapid degradation? Immediate crashing?"³¹

A few days prior to that email from Mr. Park, Mr. Chao emailed multiple colleagues and stated, *"When Todd Park and Marilyn was [sic] here yesterday one of the things Todd conveyed was this fear the WH has about hc.gov being unavailable."*³² Mr. Chao followed up with, *"He will come back again and ask on 9/30 because after knowing him for the past 3+ years I can tell when he will hang on to something for a long time."*³³

There are also several emails where Mr. Park requests or is offered briefings on a range of items related to the HealthCare.gov website. In one instance, Mr. Chao offers to provide Todd *"a walk through and demo of the online application in its current form so you can get a chance to peek under the covers of hc.gov."*³⁴ In another example, Mr. Park emails Michelle Snyder, then-Chief Operating Officer at CMS, and Henry Chao that he *"would love (with Steve [VanRoekel]) to arrange time (1 hour) in the next week and half to check in on how things are going with respect to Marketplace IT dev and testing."*³⁵ In fact, it seems as though CMS briefings to Mr. Park about development of the website were fairly commonplace as he indicates in one email to Marilyn Tavenner, *"I'm also going to visit with Henry and team for one of our evening deep-dive sessions to get up to speed on the latest status of IT and testing."*³⁶

It is difficult to reconcile Mr. Park's statement at the OGR hearing that he did not "have a really detailed knowledge base of what actually happened pre-October 1" with emails in the Committee's possession that appear to indicate otherwise.

³¹ Ibid. (Emphasis added).

³² Email from Henry Chao, Deputy CIO, CMS, to Jon Booth, CMS, et al (September 25, 2013) [HHS-0103410] (Emphasis added).

³³ Ibid. (Emphasis added).

³⁴ Email from Henry Chao, Deputy CIO, CMS to Todd Park, U.S. Chief Technology Officer, OSTP, et al (July 25, 2013) [HHS-0104905] (Emphasis added).

³⁵ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Michelle Snyder, Chief Operating Officer, CMS, et al (June 11, 2013) [HHS-0106398] (Emphasis added).

³⁶ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Marilyn Tavenner, Administrator, CMS, et al (June 26, 2013) [HHS-0106971] (Emphasis added).

Agendas and notes from the monthly Steering Committee meetings appear to further demonstrate the extent of Mr. Park's involvement and his role in putting schedule pressure on CMS to go live with the HealthCare.gov website on October 1, 2013. For instance, one meeting from May 2012 lists "Integrated Critical Path Development" as a discussion topic, and the highlight mentions that "**Todd Park reiterated the need for knowing what the critical path deadlines are, to not exceed those deadlines, and engage in a very high level of intensity and effort to assure deadlines are met.**"³⁷ Another Steering Committee meeting agenda from April 2013 states that Mr. Park "**has agreed to facilitate discussions between CMS and IRS to get several outstanding issues resolved.**"³⁸

The Committee also identified several emails that seem to contradict claims about Mr. Park not being "**substantially involved in developing or implementing security measures**"³⁹ of the website prior to its rollout. For example, in an email from Mr. Park to Mr. Chao and Ms. Snyder:

*"Attempting to integrate logos into the FFM for October 1 is not advisable. This is not because the act of integrating a logo is by itself a difficult thing to do. It's because the process for collecting health plan and product data from carriers via templates, loading these data into the HIOS system, validating the data, transferring the data from HIOS into the FFM QHP database, and having the rating engine retrieve and render that data in the FFM has been locked down, and is being utilized to support plan data collection/validation and system testing as we speak. Changing the underlying plan data template and processing routine right now – by adding a new plan data element, the logo – during the crunch-time spring we're in from now to October 1, would introduce significant risk."*⁴⁰

In April 2013, Mr. Park attended a briefing from McKinsey & Company where the group "**presented the results of a study it had been commissioned to conduct on the development of the federal exchange to the White House, HHS, and CMS officials. McKinsey briefed CMS's Chief Operating Officer, Michelle Snyder, as well as Deputy Assistant to the President for Health Policy Jeanne Lambrew and U.S. Chief Technology Officer Todd Park. McKinsey made a list of 'critical risks' to the system, including the risk that a system failure would render the marketplace unavailable.**"⁴¹

The Committee has many questions for Mr. Park as to what he did with information presented in the McKinsey briefing, including whether he briefed the President or others in the White House to ensure they had all the information they needed before deciding to continue the rollout of the HealthCare.gov website on October 1, 2013.

IV. Mr. Park's OSTP Employment and Role as HealthCare.gov Liaison to the White House

³⁷ ACA IT Exchange Steering Committee Meeting Minutes (May 17, 2012) [HHS-0110015] (Emphasis added).

³⁸ Marketplace Activities Minutes (April 5, 2013) [HHS-0109346] (Emphasis added).

³⁹ OSTP letter to SST, November 14, 2013 (Emphasis added).

⁴⁰ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Michelle Snyder, Chief Operating Officer, CMS, et al (June 25, 2013) [HHS-0106973] (Emphasis added).

⁴¹ "Red Flags: How Politics and Poor Management Led to the Meltdown of HealthCare.gov," An Inquiry by the Senate Finance Committee Minority Staff and the Senate Judiciary Committee Minority Staff, June 2014, available at: http://www.hatch.senate.gov/public/?_cache/files/e3ff7336-426b-4363-ad41-086ee120a201/HealthCare.gov%20REPORT.pdf (Emphasis added).

When Mr. Park was named the U.S. CTO in March 2012, OSTP Director John Holdren heralded his arrival from HHS by highlighting the fact that while at HHS, Mr. Park “led the successful execution of an array of breakthrough initiatives, including the creation of HealthCare.gov.”⁴²

Until he stepped down from his position on August 28, 2014, Mr. Park was featured on the ‘Leadership’ section of the OSTP website, under Director Holdren, where Mr. Park’s biography stated that his focus on “technology policy and innovation can advance the future of our nation.”⁴³

In his written testimony before the Committee on June 20, 2012, OSTP Director John Holdren explained:

“OSTP also supports me in my role as Assistant to the President for Science and Technology and the U.S. Chief Technology Officer, who sits in OSTP, in our functions advising the President on S&T dimensions of the policy challenges before the Nation, including strengthening the economy and creating jobs, improving healthcare and education, enhancing the quality of the environment, and advancing national and homeland security.”⁴⁴

On five different occasions, OSTP declined the Committee’s invitations for Mr. Park to testify in a public hearing. In a Committee hearing on March 26, 2014, Dr. Holdren had the following to say regarding Mr. Park:

“We said his involvement has not been primarily associated with the security of the site. He is not a cybersecurity expert, and the responsibility for the security of the site rested with CMS and with the interacting activities of CRS, IRS, and the SSA...”

“It has been the practice of this Administration from the beginning that assistants to the President who are not Senate-confirmed do not testify. We have other people who are experts in cyber security who are willing to testify before this Committee on cybersecurity issues. Mr. Park is not an expert in the cybersecurity aspects of the Healthcare.gov website. And he is a direct report to the President of the United States. I can’t compel him to come and testify. He doesn’t report to me.”⁴⁵

At no point during the June 2012 hearing, nor any subsequent hearing, did Dr. Holdren mention OSTP’s role or Mr. Park’s role as one of the three White House co-chairs who established the Steering Committee that helped to bring “agencies together to facilitate progress on key issues of concern and help resolve roadblocks associated with Exchange IT implementation.”⁴⁶ Mr. Park also did not mention this when questioned about his involvement with HealthCare.gov prior to its implementation in his Congressional testimony last November.

⁴² White House Blog, “Todd Park Named New U.S. Chief Technology Officer,” March 9, 2012, available at: <http://www.whitehouse.gov/blog/2012/03/09/todd-park-named-new-us-chief-technology-officer>.

⁴³ OSTP website, Todd Park bio, available at: <http://www.whitehouse.gov/administration/eop/ostp/about/leadershipstaff/park>.

⁴⁴ SST hearing, “Examining the Priorities and Effectiveness of the Nation’s Science Policies,” June 20, 2012, available at: <http://science.house.gov/hearing/full-committee-hearing-examining-priorities-and-effectiveness-nation%E2%80%99s-science-policies>. (Emphasis added).

⁴⁵ SST hearing, “A Review of the President’s Fiscal Year 2015 Budget Request for Science Agencies,” March 26, 2014, available at: <http://science.house.gov/hearing/full-committee-hearing-review-president-s-fiscal-year-2015-budget-request-science-agencies>. (Emphasis added).

⁴⁶ Email from Keith Fontenot, White House Associate Director for Health, OMB, to Todd Park, U.S. Chief Technology Officer, OSTP, et al. (Mark 8, 2013) [OSTP ACA 000582] (Emphasis added).

However, in various email exchanges, it appears that Mr. Park was intimately involved with the planning of the Steering Committee's meetings and actively participated in them. For example, in an email exchange between Bryan Sivak, HHS Chief Technology Officer, and Mr. Park, Mr. Park mentions to Mr. Sivak that they will talk about potential problems with consent through the Privacy Act that Mr. Baitman references in an earlier email, and Mr. Park says that he will make sure that Mr. Sivak is invited to future Steering Committee meetings.⁴⁷ In addition, key points from a November 2012 Steering Committee meeting noted that Mr. Park "has been engaged in discussion on NIST Level 2 inter-mechanics...CMS is moving forward with following this process, which represents SSA's understanding, as well...SSA is interested in understanding the downstream impact on the overall integrated testing, as well as the timeline."⁴⁸

In his role as U.S. Chief Technology Officer, it appears that Mr. Park was a direct liaison with various staff members in the White House as well as the President regarding the development of the HealthCare.gov website. On July 12, 2013, Mr. Chao emailed multiple CMS staffers and an employee from CGI Federal with the subject line, "*Need a write up for Todd*" and goes on to say, "*This is for sources material for Todd Park to pick nuggets from in his prep for briefing POTUS next week.*"⁴⁹ A month before the website launched, Mr. Park inquired about the possibility of Edward Siskel, then-Deputy White House Counsel and Deputy Assistant to the President, joining their call and being able to talk afterwards. Mr. Park wrote that, "*one point to discuss with him is Frank's very good point that we need to walk a fine line publicly – showing we take the risks seriously but also not baiting hackers into attacking.*"⁵⁰

In addition, Mr. Park helped communicate important cybersecurity talking points to White House staff, such as when he coordinated with top CMS and HHS staff to put together cybersecurity background points for Christopher Jennings, then-deputy assistant to the President for health policy.⁵¹ Mr. Park also participated in a background call for press in September 2013 "*with WH folks only,*"⁵² where he communicated HealthCare.gov cybersecurity points that he drafted.

V. Conclusion

It is difficult to reconcile Mr. Park's own emails relative to HealthCare.gov prior to its launch on October 1, 2013 with his testimony before the House Oversight and Government Reform Committee on November 14, 2013. The House Science, Space, and Technology Committee made repeated efforts for Mr. Park to appear in a public hearing or a transcribed briefing/interview over the course of the past year. OSTP has repeatedly blocked these requests. Given the emails provided to Congress by HHS, it appears that Mr. Park purposefully and willfully misrepresented his role and responsibilities with the HealthCare.gov website. The Administration has protected Mr. Park, who was a senior White House

⁴⁷ Email from Bryan Sivak, Chief Technology Officer, HHS, to Todd Park, U.S. Chief Technology Officer, OSTP, (January 7, 2013) [OSTP ACA 000507].

⁴⁸ Meeting Minutes, ACA IT Exchange Steering Committee, November 29, 2012. [HHS – 0110501 – HHS – 0010504].

⁴⁹ Email from Henry Chao, Deputy CIO, CMS, to Lakshmi Manambedu, CGI Federal, and et al. (July 12, 2013) [CGIHR 00168000].

⁵⁰ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Tony Trenkle, Chief Information Officer, CMS, et al. (September 3, 2013) [HHS-0106446] (Emphasis added).

⁵¹ Email from Todd Park, U.S. Chief Technology Officer, OSTP, to Christopher Jennings, Deputy Assistant to the President for Health Policy, The White House (September 3, 2013) [HHS-0106447].

⁵² Email from Todd Park, Chief Technology Officer, OSTP, to Jessica Santillo, et al. (September 17, 2013) [HHS-0105403] (Emphasis added).

official and part of the Office of Science and Technology Policy, from answering questions before the Committee about his role in the development of HealthCare.gov.

For these reasons, the Committee issued a subpoena to compel Mr. Park's appearance before the Oversight Subcommittee on November 19, 2014, one year after the Committee's first request for him to testify, to provide answers about his involvement with HealthCare.gov.

Beyond the need for public integrity and transparency, it is important to note that the estimated cost for the HealthCare.gov website to the American taxpayer is "upward of \$2 billion."⁵³ Yet, a recent U.S. Government Accountability Office on HealthCare.gov noted that, "weaknesses remain both in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls."⁵⁴ Further, in July of this year, "a hacker broke into part of the HealthCare.gov insurance enrollment website...and uploaded malicious software."⁵⁵ These are serious ongoing concerns more than a year after the website was launched, and as the next open-enrollment period approaches, the Administration needs to assure Americans that their personal information is secure on the HealthCare.gov website.

⁵³ Alex Wayne, "Obamacare Website Costs Exceed \$2 Billion, Study Finds," Bloomberg (September 24, 2014), available at: <http://www.bloomberg.com/news/2014-09-24/obamacare-website-costs-exceed-2-billion-study-finds.html>

⁵⁴ "HealthCare.gov – Actions Needed to Address Weaknesses in Information Security and Privacy Controls," GAO, September 2014, available at: <http://www.gao.gov/products/GAO-14-730>

⁵⁵ Danny Yadron, "Hacker Breached HealthCare.gov Insurance Site," Wall Street Journal (September 4, 2014), available at: <http://online.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043>

TABLE OF CONTENTS

I. PURPOSE	2
II. MISSION	2
III. SCOPE AND RESPONSIBILITIES	2
IV. MEMBERSHIP AND REPORTING STRUCTURE	4
V. ADMINISTRATION	5
VI. AGREEMENT	6

I. Purpose

This charter establishes the Affordable Care Act (ACA) IT Exchanges Steering Committee (Steering Committee) as a collaborative body and as a venue for seeking resolution of persistent interagency challenges and dependencies related to the implementation of IT exchanges in support of the Affordable Care Act.

This document outlines the mission, scope and responsibilities of the Steering Committee, identifies membership and support structures, and defines key processes and procedures. A Health Exchange Executive Secretariat (Executive Secretariat) has been established as an agent of the Committee to work with Agencies to ensure projects fully align under the Affordable Care Act in providing a streamlined and seamless interface with the American public and affected industries that will be impacted by the implementation of the health insurance exchanges under the Affordable Care Act.

II. Mission

The primary mission of the Steering Committee is to support the timely and efficient resolution of barriers while ensuring the realization of fully operational health insurance exchanges mandated under the Affordable Care Act. The Steering Committee will (a) address key Exchange information sharing policies and barriers, (b) work with Departments, Agencies, and other stakeholders as necessary on the implementation and execution of Health Insurance Exchanges.

III. Scope and Responsibilities

Steering Committee

The Steering Committee shall provide a forum for seeking resolution of interagency challenges and to further promote interagency alignments to assure the implementation of a consumer-centric health insurance exchanges under the Affordable Care Act. The Steering Committee can designate the Executive Secretariat to act on its behalf to meet these functions. The Steering Committee shall:

- Facilitate interagency discussions to promote resolution to key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government and with the state exchanges.
- Direct the formulation of work groups to identify barriers, develop or identify promising practices to support efficiencies, and develop option papers for the Committee's consideration.

- The Steering Committee will meet monthly or more frequently as deemed necessary by the Executive Secretariat, beginning in May 2012 through March 2014. The meeting frequency may be altered by the agreement of the Steering Committee Co-Chairs. Beginning in April 2014, the Steering Committee will meet on an *ad hoc* basis as advised by the Executive Secretariat or as requested by the Co-Chairs until it is the consensus of the Steering Committee members that the Exchange post-implementation issues have been sufficiently surfaced and addressed.

Executive Secretariat

The Executive Secretariat reports to the co-chaits and will support, coordinate, and act as a liaison between the Steering Committee and Departments.

The Executive Secretariat will remain operational through January 2015 or until it is the consensus of the Steering Committee members that the Exchange post-implementation issues have been sufficiently surfaced and addressed.

- Lead: HHS Program Management Office; Office of the Chief Information Officer
- Members: CMS, IRS, SSA

The Executive Secretariat's core functions will be as follows:

- Work with the designated workgroups to identify interagency IT policy issues for the Steering Committee's consideration.
- Responsible for tracking and reporting progress of individual workgroups and elevating workgroup concerns to the Steering Committee.
- Share recommendation from the Steering Committee with workgroups and Agencies; distribute and support the implementation of these recommendations.
- Work closely with Agencies and stakeholders to develop and iterate the plans for resolution of challenges as appropriate.

Agencies will continue to coordinate ACA IT exchange project governance and oversight functions within their respective organizations and work directly with their IT project teams to ensure performance and alignment with the Steering Committee recommendations as appropriate.

Working Groups

Data Sharing and Privacy

- * Objectives: Streamlining data use agreements and creating a uniform process for developing and maintaining computer matching agreements, data use agreements, ICAs, consent forms, etc.
- * Lead: Janet Miller, IRS
- * Members: HHS, SSA, DHS, VA, OPM, DoD, Peace Corps

Security Harmonization

- * Objectives: Coordinate uniform process to harmonize security and streamline negotiations/documentation of new agreements within and across each agency
- * Co-Leads: Tim May, SSA & Tom Schankweiler, CMS
- * Members: HHS, IRS, VA, DHS, Peace Corps, OPM

Operational Oversight

- * Objective: Provide a clearinghouse for issues needing to be analyzed and resolved among agencies for those issues not covered by other more specific workgroups, issue tracking and execution of common priorities in a timely/effective manner, and to assure the maximal alignment with the vision for a consumer-centric insurance exchange
- * Co-Leads: Jim Kerr, CMS, Wanda Brown (IRS)
- * Members: HHS, IRS, SSA, VA, DHS, Peace Corps, DoD, OPM

IV. Membership and Reporting Structure

The Federal Chief Information Officer (CIO), the Health Program Associate Director, and the U.S. Chief Technology Officer (CTO), in the Executive Office of the President will serve as co-Chairpersons for the Affordable Care Act IT Steering Committee. Membership will be comprised of senior executives from each of the participating Departments and Agencies who understand the ACA and health insurance exchange-related IT and business/mission needs of their Departments and Agencies and who can make key policy and management judgments on behalf of the respective Departments.

The following Departments and Agencies are represented on the Committee and will designate a senior executive as described above as members of the Steering Committee:

- Department of Health & Human Services, Centers for Medicare and Medicaid Services
- Department of Treasury, Internal Revenue Service
- Department of Homeland Security
- Department of Defense
- Department of Veterans Affairs

- Social Security Administration
- Peace Corps

Additional members may be added if additional interagency dependencies are identified.

Representatives from other Departments and offices, including subject matter experts (SMEs) and other advisors, may be invited to attend Steering Committee meetings with the concurrence of the Steering Committee co-Chairs.

V. Administration

A. Meetings

The Steering Committee shall meet as needed and as advised by the Executive Secretariat. Meetings may be in person, by conference-call, or other "virtual" meeting tools. Materials shall be distributed to the members prior to the meeting in order for the members to have adequate time to review and consider the material. The members will be requested to review and provide comment/feedback on materials as appropriate.

B. Records Management

The Executive Secretariat will be responsible for appointing a designee to distribute materials prior to and post meetings (i.e., agenda, meeting minutes).

VI. Agreement

Steven VanRoekel, Executive Office of the President Date

Keith Fontenot, Executive Office of the President Date

Todd Park, Executive Office of the President Date

Donna Roy, Department of Homeland Security Date

Robert Carey, Department of Defense Date

Frank Baitman, Department of Health & Human Services Date

Marilyn Tavenner, HHS / Centers for Medicare & Medicaid Services Date

Joshua Andrews, Peace Corps Date

Bea Disman, Social Security Administration Date

Terry Milholland, Department of Treasury/IRS Date

Alan Constantian, Department of Veterans Affairs Date

Message

From: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent: 8/29/2013 1:39:35 AM
To: Trenkle, Tony (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]
CC: Baitman, Frank (OS/ASA/OCIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Frank.Baitman.OS]; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Mielke, Dawn M. [Dawn_M._Mielke@ostp.eop.gov]; Graubard, Vivian [Vivian_P_Graubard@ostp.eop.gov]; Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana.Khalid.CMS]; Charest, Kevin (OS/ASA/OCIO/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=he17]
Subject: Re: Cyber next steps

Terrific, Tony, thanks, looking forward to it!

Todd

From: Trenkle, Tony (CMS/OIS) [mailto:tony.trenkle@cms.hhs.gov]
Sent: Wednesday, August 28, 2013 09:37 PM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) <Frank.Baitman@hhs.gov>; Snyder, Michelle (CMS/OA) <Michelle.Snyder@cms.hhs.gov>; Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA) <Aryana.Khalid@cms.hhs.gov>; Charest, Kevin (OS/ASA/OCIO/OIS) <Kevin.Charest@hhs.gov>
Subject: Re: Cyber next steps

I think that we all can agree on that. Todd, the call will follow the outline that you laid out in your email and our discussion should then drive what we say in the memo.

On Aug 28, 2013, at 7:38 PM, "Park, Todd" <Todd_Y_Park@ostp.eop.gov> wrote:

OK, will try to call in for a 10 am Wed meeting and make that work. And Frank, agree with your points about public-facing material.

Thanks,

Todd

From: Baitman, Frank (OS/ASA/OCIO) [mailto:Frank.Baitman@hhs.gov]
Sent: Wednesday, August 28, 2013 7:24 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cyber next steps

+ Adding Kevin

Todd et al,

Unfortunately the Secretary's Leadership Council is next Wed afternoon – and believe we'll have some IT items on the agenda, so I need to be there.

I believe we can address our defenses in a balanced manner: it should come as no surprise that we experience attacks and have defenses. But, for public facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage.

- Frank

From: <Park>, Todd <Todd_Y_Park@ostp.eop.gov>
Date: Wednesday, August 28, 2013 6:44 PM
To: "Trenkle, Tony (CMS/OIS)" <tony.trenkle@cms.hhs.gov>
Cc: "Snyder, Michelle (CMS/OA)" <Michelle.Snyder@cms.hhs.gov>, "Mielke, Dawn M." <Dawn_M_Mielke@ostp.eop.gov>, "Graubard, Vivian" <Vivian_P_Graubard@ostp.eop.gov>, Frank Baitman <frank.baitman@hhs.gov>, "Khalid, Aryana C. (CMS/OA)" <Aryana.Khalid@cms.hhs.gov>
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- <!--[if !supportLists]--><!--[endif]-->There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo – will try to set up time with him for Thursday the 5th)
- <!--[if !supportLists]--><!--[endif]-->It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- <!--[if !supportLists]--><!--[endif]-->Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
 Todd

From: Trenkle, Tony (CMS/OIS) [mailto:tony.trenkle@cms.hhs.gov]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:Todd.Y.Park@ostp.eop.gov]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. <!--[if !supportLists]--><!--[endif]-->We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there – to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later – looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!
2. <!--[if !supportLists]--><!--[endif]-->You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others – we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi – for internal use only.
3. <!--[if !supportLists]--><!--[endif]-->I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace – we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

Message

From: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent: 8/28/2013 10:44:53 PM
To: Trenkle, Tony (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]
CC: Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Mielke, Dawn M. [Dawn_M_Mielke@ostp.eop.gov]; Graubard, Vivian [Vivian_P_Graubard@ostp.eop.gov]; Baitman, Frank (OS/ASA/OCIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Frank.Baitman.OS]; Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana.Khalid.CMS]
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo – will try to set up time with him for Thursday the 5th)
- It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
 Todd

From: Trenkle, Tony (CMS/OIS) [mailto:tony.trenkle@cms.hhs.gov]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Wednesday, August 28, 2013 9:45 AM

2. We had already included the SANS award into the internal memo, however, we are expanding the explanation about the CMS continuous monitoring capabilities and how they have now been expanded to the marketplace systems.
3. Yes, Teresa and Mike will join the Palantir call.

From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Wednesday, September 04, 2013 12:33 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Baitman, Frank (OS/ASA/OCIO); Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Follow up to this morning's call

Tony, great job to you, Frank and team on the call -- it was very productive and helpful. Your next steps sound exactly right. Three additional questions/notes:

1. What is the best and most efficient way to prep and utilize MITRE as an external validator? Would it be to give them a copy of the internal memo, under cone of titanium silence, and ask them to be ready to speak to external folks before or after the hearing about the general soundness of the approach CMS is taking? Would it be appropriate to touch base with them this week about serving as an external validator, so we can confirm that they are willing to do this?
2. Thoughts on integrating a couple of sentences about the external award CMS received for its monitoring work into either the internal memo or the external Q and A?
3. On the Palantir call, my thought is to ask them to assume the role of a general cyber sounding board, ask them what they would be most worried about if they were us, and how they would think about defense/mitigation. Sound OK? And will you and Frank have your CISO team join?

Thanks so much!
 Todd

From: Trenkle, Tony (CMS/OIS) [<mailto:tony.trenkle@cms.hhs.gov>]
Sent: Wednesday, September 04, 2013 11:59 AM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) <Frank.Baitman@hhs.gov>; Tavenner, Marilyn (CMS/OA) <Marilyn.Tavenner@cms.hhs.gov>; Khalid, Aryana C. (CMS/OA) <Aryana.Khalid@cms.hhs.gov>; Snyder, Michelle (CMS/OA) <Michelle.Snyder@cms.hhs.gov>; Fryer, Teresa M. (CMS/OIS) <Teresa.Fryer@cms.hhs.gov>; Mellor, Michael (CMS/OIS) <Michael.Mellor@cms.hhs.gov>; Charest, Kevin (OS/ASA/OCIO/OIS) <Kevin.Charest@hhs.gov>; Trenkle, Tony (CMS/OIS) <tony.trenkle@cms.hhs.gov>
Subject: Follow up to this morning's call

Todd,

I thought the call went well and hopefully it responded to Ed Siske's concerns as well as yours. Here is a summary of next steps. I am also copying Michelle and Marilyn to keep them informed.

1. CMS will prepare an internal memo that discusses our security marketplace security preparations and operational plan of action. The memo will focus on the following areas in some detail, but will not discuss specific product names:
 - a. Preparations for and defenses against cyber-attack-this will discuss specific marketplace work as well as the overall CMS IT security infrastructure
 - b. Response/actions in the event of an attack/crisis-Also will discuss marketplace specific and how that ties into our current response planning.
 - c. Coordination with the HHS IG on potential prosecutions-This will only focus on our initial handoff to the IG, not what occurs after that.

Frank and Kevin will add detail on how HHS provides additional overall support. The memo will be distributed to a limited internal Government audience, to be coordinated through you. We discussed that one way of sending the memo would be to address it from me to Frank. A draft of the memo is being developed and will need to be vetted with Michelle and Marilyn. I assume that Frank will handle any Departmental communications with assistance from us as needed. We will attempt to have the memo available by COB Friday, depending on clearance.

2. On a separate but related track, we will work with Frank to develop generic Q&As that could be made public. These will not address specifics of CMS internal security infrastructure but would focus on overall government security measures, that the Marketplace would adhere to. These could potentially be given to minority House members before the 9/11 hearing. We are sensitive to the fact that these Q&As be kept generic and not draw hackers' attention. We will also try to have these done by the end of the week.
3. We agreed that for external validation, Mitre would be the most logical choice, given their long-track record of working with multiple Federal agencies and their overall knowledge of the IT security industry, including private sector security measures. We agreed that other external organizations would not have the depth of business and technical knowledge to provide a good validation without diverting CMS resources needed to finish the testing.
4. We will speak with the Palantir folks today at 4 but will keep the discussion high-level, recognizing that they are not an appropriate choice to be an external validator.

Others, please add if I have missed anything.

Tony

Appointment

From: Laura_E_Lynch@omb.eop.gov [Laura_E_Lynch@omb.eop.gov]
Sent: 8/21/2012 9:35:19 PM
To: VanRoekel, Steven [Steven_L_VanRoekel@omb.eop.gov]; Callaghan, Liz M. (OS/ASA/OCIO); Martin, Kathryn; Tran-Lam, Minh-Hai; Bales, Carol A.; Ple-Plakon, Alisa; Reczek, Jeff; Trenkle, Tony (CMS/OIS); Chao, Henry (CMS/OIS); 'jeremy.grant@nist.gov'; 'deborah.gallagher@gsa.gov'; Lynch, Laura; Lefkowitz, Naomi B. (naomi.lefkowitz@nist.gov); Williams, Sonji (CMS/OIS); Schlosser, Lisa; Fontenot, Keith J.; Park, Todd; Baitman, Frank (OS/ASA/OCIO); Overstreet, Tyler J.; Mostashari, Farzad (HHS/ONC); Rice, M. David; Pritts, Joy (HHS/ONC); Welling, Erum; Zhen, Changqing
Subject: Copy: ACA NSTIC Meeting
Location: Eisenhower Room, WHCC
Start: 8/31/2012 2:30:00 PM
End: 8/31/2012 3:30:00 PM
Show Time As: Busy

All – please find the deck for this meeting attached. *Thanks, Laura*

This is a technical briefing with CMS for an update on their identity management work for the ACA Exchanges. With the meeting taking place in the White House Conference Center, no waves is needed.

Appointment

From: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent: 6/14/2013 2:59:12 PM
To: Park, Todd [Todd_Y_Park@ostp.eop.gov]; Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS); VanRoekel, Steven; Lynch, Laura; Tran-Lam, Minh-Hai; Ple-Plakon, Alisa; Sivak, Bryan (HHS/IOS); Baitman, Frank (OS/ASA/OOO); Kendall, Damaris (HHS/OS); Armstead, Andrea E. (CMS/OA); Seth, Sharman M. (CMS/OA); Reczek, Jeff; Overstreet, Tyler J.; Martin, Kathryn; Williams, Claudia; Schlosser, Lisa
Subject: Copy: ACA Sync-up
Location: [REDACTED]
Start: 6/26/2013 2:00:00 PM
End: 6/26/2013 3:00:00 PM
Show Time As: Busy

From: Park, Todd
Sent: Tuesday, June 11, 2013 07:52 PM
To: michelle.snyder@cms.hhs.gov <michelle.snyder@cms.hhs.gov>; henry.chao@cms.hhs.gov <henry.chao@cms.hhs.gov>
Cc: marilyn.lavanner@cms.hhs.gov <marilyn.lavanner@cms.hhs.gov>; VanRoekel, Steven; Graubard, Vivian; Lynch, Laura
Subject: Sync-up
 Hi Michelle and Henry, hope all is terrific with you!

As you've heard from Marilyn, would love (with Steve) to arrange time (1 hour) in the next week or week and half to check in on how things are going with respect to Marketplace IT dev and testing. (And also to discuss the tactical question of issuer logos). Would love to arrange a visit to Baltimore, but given how crazy schedules are, I'm guessing that a videoconference or conference call would be more feasible.

We don't need any special documentation or whatnot. Just you ☺ If you have something that you've already put together for another purpose that you'd like to send, great.

May Vivian and Laura work with your office to set up a time to chat?

Cheers,
Todd

Message

From: Baitman, Frank (OS/ASA/OCIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=FRANK.BAITMAN.OS]
Sent: 4/12/2013 3:14:35 PM
To: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Subject: FW: Meeting with the National Security Staff and OMB
Attachments: image002.jpg

Todd, here's the note from Michael Daniel.

Would you want to follow up with him to get more details on the objective of the meeting? Tony and I chatted about it this morning, and we're concerned that there'll be a push to make ACA identity proofing NSTIC compatible from the start: that's definitely on our roadmap, but as we discussed, that needs to be v.2. (In fact, that point has been made at previous WH meetings.)

Thanks,
- Frank

From: Caddy, Cheri [mailto:Cherlene_G_Caddy@nss.eop.gov]
Sent: Thursday, April 11, 2013 6:03 PM
To: Holland, Ned (HHS/ASA); Trenkle, Tony (CMS/OIS)
Cc: Daniel, J. Michael; Orment, Andy; Jeremy.Grant@nist.gov; Lefkowitz, Naomi B. (naomi.lefkowitz@nist.gov); VanRoekel, Steven; Davlin, Jessica
Subject: Meeting with the National Security Staff and OMB

Mr Holland and Mr Trenkle,

Michael Daniel would like to meet with you on 23 April at 3pm at the White House to discuss CMS plans for user credentialing and identity proofing in its implementation of the Affordable Care Act. Could you please confirm your availability for this time, or provide a scheduling POC whom we can work with?

Thanks for your help,

Cheri Caddy

Director for Cyber Policy Integration and Outreach

National Security Staff

Executive Office of the President



Commercial: [REDACTED]

Secure: [REDACTED]

<Cheryl.Campbell@...>; 'Hemant.Sharma@...'; Hemant.Sharma@...
 'Rich.Martin@...'; 'Rich.Martin@...'; Van, Hung B. (CMS/OIS)
 Subject: RE: Discussion points

I believe Hemant & CGI needs to address those questions based on the Performance testing run last night.

We'll be continue to test today, tomorrow & beyond until we reach at least 10k concurrent users, and eventually 50k. So far, we only covered the individual application in PST, and today we'll be focusing on scripting Plan results, Plan compare, and enrollments. Also we'll be performance testing FPM-EIDM integration today.

-----Original Message-----

From: Chao, Henry (CMS/OIS)
 Sent: Sunday, September 29, 2013 8:43 AM
 To: Thurston, Robert (CMS/CTR); Zaman, Akhtar (CMS/OIS); Outerbridge, Monique (CMS/OIS);
 'George.Schindler@...'; 'Cheryl.Campbell@...'; 'Hemant.Sharma@...';
 'Rich.Martin@...'; Van, Hung B. (CMS/OIS)
 Subject: Fw: Discussion points

These are Todd's questions.

Henry Chao
 Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare
 & Medicaid Services
 7500 Security Blvd
 Baltimore, MD 21244
 (Fm)
 (At)
 (88)

----- Original Message -----

From: Park, Todd [mailto:Todd_Y_Park@estp.eop.gov]
 Sent: Sunday, September 29, 2013 08:23 AM
 To: Chao, Henry (CMS/OIS)
 Cc: Snyder, Michelle (CMS/DA)
 Subject: Discussion points

Hi Henry, channeling my inner Michelle, a few questions (all of which I think she or I have floated at some point), perhaps for discussion at the 9 am or later today:

-- Has the team run performance/diagnostic testing on the whole FPM, so that we know that the MarkLogic bottleneck is in fact the critical, rate-limiting one, as opposed to another bottleneck in, say, Plan Compare or elsewhere, that could also constrain the number of concurrent users?

-- In other words, does the performance testing the team is doing make you confident that the FPM across the board can indeed take 16,000 concurrent users, rising to 60,000-70,000 with the new hardware? - So far we were able to run 2000 concurrent users in SMP3B, Hemant needs to

-- Are we going to run performance testing today and tomorrow on the growing aggregate collection of hardware (not just one unit of it), so we validate the projections of 16,000/60,000-70,000 with the actual production machinery?

-- Are we testing to make sure that incoming traffic gets properly load balanced across the VMs/units? (This may be accomplished by the previous item)

-- What happens after the 16,000/60,000-70,000 threshold is reached? Is there gradual degradation of response time for users? Rapid degradation? Immediate crashing?

Massive kudos again for the incredible progress the team is making!
 This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic mail or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify the sender by reply email and delete the original message (including any attachments) in its entirety.

Message

From: Chao, Henry (CMS/OIS) [/O=HHS EES/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=HENRY.CHAO.OS]
Sent: 9/25/2013 8:53:00 PM
To: Booth, Jon G. (CMS/OC) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=jon.booth.cms89225837];
 Patel, Ketan (CMS/DC) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=ketan.patel.cms12902361];
 Linares, George E. (CMS/OIS) [/O=HHS EES/OU=First Administrative
 Group/cn=Recipients/cn=george.linares.cms36441481]; Skinner, Dennis R. (CMS/OIS) [/O=HHS EES/OU=First
 Administrative Group/cn=Recipients/cn=dennis.skinner.cms96729034]; Royle, Erick B. (CMS/OIS) [/O=HHS
 EES/OU=First Administrative Group/cn=Recipients/cn=erick.royle.cms58397202]; Sharma, Hemant (CGI Federal)
 (Hemant.Sharma [REDACTED]); (Hemant.Sharma [REDACTED]); Keith Rubin (Keith Rubin [REDACTED])
 Margush, Doug C. (CMS/OIS) [/O=HHS EES/OU=First Administrative
 Group/cn=Recipients/cn=doug.margush.cms34349421]; Kariton Kim (kkim [REDACTED])
 Schankweiler, Thomas W. (CMS/OIS) [/O=HHS EES/OU=First Administrative
 Group/cn=Recipients/cn=Thomas.Schankweiler.PSC]
CC: Outerbridge, Monique (CMS/OIS) [/O=HHS EES/OU=First Administrative
 Group/cn=Recipients/cn=Monique.Outerbridge.OS]; Kariton Kim (kkim [REDACTED]); Rich Martin
 (Rich.Martin [REDACTED]) (Rich.Martin [REDACTED]); Oh, Mark U. (CMS/OIS) [/O=HHS EES/OU=EXCHANGE
 ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Mark.Oh.OS]; Thurston, Robert (CMS/CTR)
 [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Robert.Thurston.CMS]; Um, Peter (CMS/CTR)
 [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP
 (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Peter.Um1.CMS@ees.hhs.gov97f]; Raddliffe, Glenn D. (CMS/OIS) [/O=HHS
 EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Glenn.Raddliff.OS]; Sharma,
 Hemant (CGI Federal) (Hemant.Sharma [REDACTED]) (Hemant.Sharma [REDACTED]); Keith Rubin
 (Keith.Rubin [REDACTED]); Coutts, Todd (CMS/OIS) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP
 (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Todd.Coutts1.CMS@ees.hhs.gov33a]; Basavaraju, Venkat (CMS/OIS)
 [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Venkat.Basavaraju.CMS]; Driscoll, Adam (CMS/OIS)
 [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Adam.Driscoll.CMS]; Berkley, Katrina (CMS/OIS)
 [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=katrina.layne.cms86157767]; Trenkle, Tony
 (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]; Carter, Cathy
 T. (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=cathy.carter.cms72924149]; Gass,
 Carole F. (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=carole.gass.cms68688311];
 Hogle, Mark P. (CMS/OIS) [/O=HHS EES/OU=First Administrative
 Group/cn=Recipients/cn=mark.hogle.cms61781245]; Peel, Nydia M. (CMS/OIS) [/O=HHS EES/OU=First
 Administrative Group/cn=Recipients/cn=nydia.peel.cms9367865]; Walter, Stephen J. (CMS/OIS) [/O=HHS
 EES/OU=First Administrative Group/cn=Recipients/cn=stephen.walter.cms38487876]; Margush, Doug C. (CMS/OIS)
 [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=doug.margush.cms34349421]; Stevenson, Corey B.
 (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=corey.stevenson.cms89401876]; Gray,
 Edward M. (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=edward.gray.cms04960864];
 Plaugher, Mark I. (CMS/OIS) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP
 (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Mark.Plaugher1.CMS]; Skinner, Dennis R. (CMS/OIS) [/O=HHS
 EES/OU=First Administrative Group/cn=Recipients/cn=dennis.skinner.cms96729034]; Royle, Erick B. (CMS/OIS)
 [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=erick.royle.cms58397202]; Fletcher, John A.
 (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=john.fletcher.cms53745823]; Trudel,
 Karen (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=karen.trudel1.cms64372368]
Subject: RE: CGI Deployment Notification - E&E TEST2 Tuesday\Wednesday September 24\25 R7.0.0.9.10 Build 179
Importance: High

Jon, Ketan, and George—When Todd Park and Marilyn was here yesterday one of the things Todd conveyed was this fear the WH has about hc.gov being unavailable. I explained about the Akamai piece and the split between learn and get insured sides so he was satisfied for the moment. He will come back again and ask on 9/30 because after knowing him

HHS-0103410

for the past 3+ years I can tell when he will hang on to something for a long time. Todd does have a good point and I think we should have a more comprehensive answer as to how we will ensure high availability. I think this discussion includes the shared services as well.

George—can I ask you to lead a discussion on HA across the board with ensuring we have everything aligned with the demand for 99.99% uptime on HC.gov (or at least the learn side as a minimum, including Spanish learn) and all of the dependencies with Security, Akamai, TMRK Internet facing bandwidth and redundancies, security early warning and monitoring, Shared Services, and CGI, QSSI, and CACI operations. Todd is conducting takeover reviews and some of that is complementary to a HA plan.

Dennis and Erick—would you please document this and capture the ops aspect of HA and execution of monitoring to ensure all the dependencies have early warning monitoring of degradation and/or signs where we have to take the site down and/or bounce the servers? Please put it in to an ops document format like an SOP and do the necessary changes needed for the monitoring tools. Perhaps Yousef can assist here.

Jon and Ketan—can you think about a better way to convey to the public when the site is not available? I am picturing in my mind all the major print and online publications taking screenshots of what is below and just ramping up the hyperbole about hc.gov not functional.

Let me know if you have questions.

Thanks

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[REDACTED]

From: Manik Naik [mailto:mnaik@[REDACTED]]
Sent: Wednesday, September 25, 2013 3:04 PM
To: Bartolotti, Larry (CGI Federal); Van, Hung B. (CMS/OIS); Shannon, Andrew (CGI Federal); Margush, Doug C. (CMS/OIS); Kutsilev, Lubo (CGI Federal); Neldecker, Bob (CGI Federal); O'Mara, Katelynne J (CGI Federal); Oh, Mark U. (CMS/OIS); Dill, Walter (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Carter, Cheryl K (CGI Federal); Deepak Bhatta; Walker, Benjamin L. (CMS/CCIIO); Zaman, Akhtar (CMS/OIS); Winthrop, Monica (CGI Federal); Martin, Rich (CGI Federal); Chao, Bing (CMS/OIS); Jagadish Gangahanumaiah; Kariton Kim; Maenner, Kristine S. (CMS/OEM); Miller, Daniel J. (CMS/OIS); Shao, Lijun (CMS/CPI)
Cc: James, Brian M. (CMS/CCIIO); Thompson, Tyrone (CMS/OIS); Walter, Stephen J. (CMS/OIS); Shropshire, Richard (CMS/CCIIO); Cummings, Duane (CGI Federal); Thurston, Robert (CMS/CTR); 'peter [REDACTED]'; De Moura, Jesse (CGI Federal); FFM-Build Deployment; Calem, Mark (CGI Federal); Sharma, Hemant (CGI Federal); Halkedis, John (CGI Federal); Kodavakuru, Radha (CGI Federal); Sousa, Steven (CGI Federal); Banerjee, Dharitri (CGI Federal); 'bjones [REDACTED]'; Pradeep Jain; Pankaj Shelkhatwat; Dinakaran, Sai (CGI Federal); Sean McHale; Devkinandan Salvi;
Chao, Henry (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Subject: RE: CGI Deployment Notification - E&E TEST2 Tuesday\Wednesday September 24\25 R7.0.0.9.10 Build 179

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Tuesday, July 30, 2013 09:43 PM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA)
Subject: RE: Walk through of the online application in hc.gov

Hi Henry and Michelle, just circling back on the below, to see what general date range you think might make sense for this visit -- would next week work? Just need to have a bit of advance time to line up Julian and David's schedules (and I'm out the week of August 12-16). Also: if you want to cut down on the time of the visit, ratcheting it down to something more like 60-90 minutes, or modify the agenda in any way, just let me know....

Thoughts? Thanks!
Todd

----- Original Message -----

From: Park, Todd
Sent: Thursday, July 25, 2013 3:01 PM
To: 'henry.chao@cms.hhs.gov'
Cc: 'Michelle.Snyder@cms.hhs.gov'
Subject: Re: Walk through of the online application in hc.gov

Hi Henry, thanks so much! To provide more context, as I shared with Michelle, I'll be bringing David Simas and Julian Harris (Keith Fontenot's successor, newly arrived) with me. Would love to (1) walk through the current live online workflow (ideally from the start of the application through Plan Compare and selection) and (2) provide the opportunity for Julian to get the latest update on (a) IT dev, (b) testing, and (c) operational prep.

For (2), Julian is interested in one level of detail below the POTUS presentation. I would not prepare any custom materials whatsoever for the meeting, but it would be great to show him (a) the slide you showed me with all of the IT modules/completion dates, (b) the testing summary for fed agencies, states, issuers you wrote up recently (i think for someone's testimony), or similar material, and (c) a slide (if you have it) of key operationalization steps (high level) on the road to Oct 1 and Dec 1 (e.g., contract X let, center X live, etc.).

Both Julian and David took great pains to ask that the visit not be disruptive to your work -- I think that the message to give y'all the space to rock and roll is spreading :)

So I'm thinking a focused two-hour visit, in Baltimore, going thru the live workflow, and using high-level materials you already have.

Would next week be best, or would the week after be better, or would either week be fine? I haven't yet pinged David and Julian for their availability, but wanted to see what was optimal for you first. It would be good to combine both of their visits, to save you time. Thoughts on timing?

Michelle, it would be terrific for you to join -- would be great for you to meet Julian and David, both of whom are terrific; and I've told both of them that you and Henry are pure awesomeness :)

Thanks!
Todd

----- Original Message -----

From: Chao, Henry (CMS/OIS) [mailto:henry.chao@cms.hhs.gov]

Sent: Thursday, July 25, 2013 09:53 AM

To: Park, Todd

Cc: Oh, Mark U. (CMS/OIS) <mark.oh@cms.hhs.gov>; Coutts, Todd (CMS/OIS)

<Todd.Coutts1@cms.hhs.gov>; Outerbridge, Monique (CMS/OIS)

<monique.outerbridge@cms.hhs.gov>; Grothe, Kirk A. (CMS/OIS)

<kirk.grothe@cms.hhs.gov>; Berkley, Katrina (CMS/OIS)

<katrina.berkley@cms.hhs.gov>; Rhones, Rhonda D. (CMS/OIS)

<Rhonda.Rhones@cms.hhs.gov>; Graubard, Vivian;

'rich.martin [REDACTED]' <rich.martin [REDACTED]>;

'cheryl.campbell [REDACTED]' <cheryl.campbell [REDACTED]>;

'Lakshmi.Manambedu [REDACTED]' <Lakshmi.Manambedu [REDACTED]>;

'Mark.Calem [REDACTED]' <Mark.Calem [REDACTED]>;

'Paul.Weiss [REDACTED]' <Paul.Weiss [REDACTED]>; Wallace, Mary H.

(CMS/OC) <Mary.Wallace@cms.hhs.gov>; Booth, Jon G. (CMS/OC)

<Jon.Booth@cms.hhs.gov>

Subject: Walk through of the online application in hc.gov

Todd,

If you recall we had agreed to provide you a walk through and demo of the online application in its current form so you can get a chance to peek under the covers of hc.gov.

Michelle mentioned you contacted her about this and that I should follow-up with you to schedule the walk through.

Katrina can work with Vivian to find a window of opportunity next week if you agree.

Let us know.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director Office of
Information Services Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244

██████████ (Pri)
██████████ (Alt)
██████████ (BB)

Message

From: Tavenner, Marilyn (CMS/OA) [/O=HHS EES/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MARILYN.TAVENNER.CMS]
Sent: 6/26/2013 9:55:47 PM
To: 'Todd_Y_Park@ostp.eop.gov' [Todd_Y_Park@ostp.eop.gov]; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.OIS]
CC: Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana.Khalid.CMS]
Subject: Re: Follow-up

Thanks Todd. Appreciate the help as always!!!!

From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Wednesday, June 26, 2013 05:34 PM
To: Tavenner, Marilyn (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Follow-up

Hi Marilyn, Michelle, and Henry,

After talking with Henry and team, I spoke with Mark about the logo issue, and explained why attempting to add logos for October 1 is extremely unwise. He understands. He may want me to get on the phone with someone from the Blues so they fully understand it. I'm more than happy to do so on your behalf – this issue should not consume any more of your time.

Marilyn, I'm also going to visit with Henry and team for one of our evening deep-dive sessions to get up to speed on the latest status of IT and testing – during the week of July 8. Michelle, Henry, and I had a check-in call today, but I think that Henry is right that to really understand current status and next steps, there is no substitute for an evening deep-dive. So I'll bring healthy food and snacks to Baltimore and camp out with Henry and team for a few hours ☺

All the best,
Todd

Meeting Minutes

Subject	ACA IT Exchange Steering Committee	Date	May 17, 2012
Facilitator	Ron Thompson, HHS PMO	Time	10- 11:00 AM
Location	233 EEOB	Scribe	Christi Dant, HHS PMO
Steering Committee Members	<p>Steering Committee Co-Chairs, Executive Office of the President:</p> <ul style="list-style-type: none"> • Steven VanRoekel • Keith Fontenot • Todd Park <p>Steering Committee Members:</p> <ul style="list-style-type: none"> • Frank Baitman, HHS • Alan Constantian, VA • Terence Milholland, IRS • Beatrice Disman, SSA • Dorine Andrews, Peace Corps • Donna Roy, DHS – Not Present • Marilyn Tavenner, CMS – Not Present • Robert Carey, DOD – Not Present 		
Attendees	<p>Maryann Rockey, DOD; Tony Trenkle, CMS; John Teeter, HHS; Minh-Hai Tran-Lam, OMB; Ronald Thompson, HHS; Tim May, SSA; Christi Dant, HHS; Jason Levitis, IRS; Gina Garza, IRS; Staccardo Washington, IRS; Monique Outerbridge, CMS; Marty Pippins, IRS; Lisa Schlosser, OMB; Jeffrey Reczek, OMB; Alisa Ple-Piakon, OMB; Kathryn Martin, OMB; Tyler Overstreet, OMB; M. David Rice, OMB; Kristin Rzeczkowski, OMB</p>		

Key Points Discussed		
No.	Topic	Highlights
1.	Charter	Comments incorporated. Still needs to be signed.
2.	Executive Secretariat Updates	Workgroups are coming together. PaDS & Security have met twice. Exec Sec & WG leads have daily calls. Not all workgroups have representation from all Agencies (See action items 1 & 4 below)
3.	Workgroups Reports	Privacy & Data Sharing (PaDS): Tim May briefed on status of combined federated ID management solution. Identity Management is a part of the package and is designed around NSTIC policy standards; also driving toward coordinating one unified review with the states, using one set of documents.

Key Points Discussed		
No.	Topic	Highlights
	Workgroup Reports cont.	<p>Security Harmonization (SH): Janet Miner provided Ecosystem presentation developed between CMS & IRS that can serve as basis for federated model. Holistic eco-system view will be developed including all federal partners. One early byproduct of WG collaboration is an interest in collaborating on oversight, combined site visits for auditing.</p> <p>Operational Oversight (OO): SSA requested that Hours of Operation (24/7) issue be fast tracked for resolution before end of June. Keith Fontenot suggested that a Service Level Agreement might be a starting point (AI-8). The workgroup needs additional membership and will prioritize this and the completion of the integrated critical path development (AI-10).</p>
4.	Integrated Critical Path Development	<p>Steering Committee co-chairs reinforced the need to develop integrate critical path ASAP. Monique Outerbridge (CMS) described a number of existing efforts nearing completion that will be used to inform this deliverable (AI-10).</p> <p>Todd Park reiterated the need for knowing what the critical path deadlines are, to not exceed those deadlines, and engage in a very high level of intensity and effort to assure deadlines are met.</p>
5.	Discussion on Next Steps	Meeting Frequency: Monthly standing meeting will be set. Scheduled will be revised as appropriate. Duration: Through 2014.

Action Items			
No.	Action Item(s)	Owner	Target Date
Previous Action Items			
AI-1	Agencies to provide points of contact for both Security Harmonization & Data Sharing and Privacy Workgroups	SC Members	Overdue DOD *Executive Secretariat requested OPM representation
AI-2	Combined Security Harmonization & Data Sharing and Privacy Workgroups to hold first meeting	PaDS & SH WG	Completed 5/8/12
AI-3	Workgroup co-leads attended NASCIO/CIO Council meeting	PaDS & SH WG	Completed 5/9/12
AI-4	Agencies provided points of contact for	SC Members	Overdue

No.	Workstream	Status
		<ul style="list-style-type: none"> This could result in multiple awards to support these requirements geographically. Question: Will this contract support States enrolled in State-Based Marketplaces (SBM) or just States enrolled in the Federally-Facilitated Marketplace (FFM) and State-Partnership Marketplaces (SPM)? <p>B. Navigator Grants</p> <p>Status:</p> <ul style="list-style-type: none"> Navigator Grant FOA was released on Tuesday, 4/9. Grants are scheduled to be awarded in August.
4	External Agencies	<p>A. Agencies Requesting Funding</p> <ul style="list-style-type: none"> We've received the following requests for funding: <ul style="list-style-type: none"> OPM: \$76,000 initial build & \$16,000 a year for maintenance VA: \$700,000 (0.12 per transaction fee) Total known 2013 costs are \$776,000 and future annual estimated costs are \$716,000 (assuming transactions don't increase drastically -- we don't have an estimate of future transaction levels). DoD may request funding as well, but we haven't received a formal request. There was a prior decision to not allow these types of request for funds. We have no idea if we'll receive similar requests in the future. A decision on whether or not to uphold the prior decision is needed before we can proceed. <p>B. Issues Being Negotiated with IRS</p> <ul style="list-style-type: none"> Todd Park has agreed to facilitate discussions between CMS and IRS to get several outstanding issues resolved. CMS' issues are: <ul style="list-style-type: none"> ID Proofing (Shared Secrets)—Replace the Adjust Gross Income (AGI) question with a question related to whether or not a tax refund was received in a specified tax year

Message

From: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent: 6/26/2013 2:03:17 AM
To: Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS];
 Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.US]
Subject: RE: Draft writeup

Is it possible to get any edits/corrections/additional detail by COB Thursday?

Would love to loop back with Jeanne and Mark on Friday before I head out for (an attempted) vacation from July 1 to July 5. I gave Jeanne a heads up today to telegraph what's coming.

I think that the key will be to give Jeanne and Mark a bulletproof set of talking points they can use to push back in their conversations with the Blues and have the Blues truly understand why the logo play is a bad idea right now. (I don't think the Blues really understand that yet).

From: Snyder, Michelle (CMS/OA) [mailto:Michelle.Snyder@cms.hhs.gov]
Sent: Tuesday, June 25, 2013 5:48 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Subject: RE: Draft writeup

Looks good.....

A. Michelle Snyder
 Deputy Chief Operating Officer
 DHHS/CMS


From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Tuesday, June 25, 2013 1:13 AM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Draft writeup

Please keep close hold -- loop in folks who can help with the details, but don't circulate broadly yet, if you don't mind. Let me know if this sounds right -- any corrections/edits/additions/deletions welcome:

Attempting to integrate logos into the FFM for October 1 is not advisable. This is not because the act of integrating a logo is by itself a difficult thing to do. It's because the process for collecting health plan and product data from carriers via templates, loading these data into the HIOS system, validating the data, transferring the data from HIOS into the FFM QHP database, and having the rating engine retrieve and render that data in the FFM has been locked down, and is being utilized to support plan data collection/validation and system testing as we speak. Changing the underlying plan data template and processing routine right now -- by adding a new plan data element, the logo -- during the crunch-time sprint we're in from now to October 1, would introduce significant risk. Think of it as trying to change a gear in an airplane engine in mid-flight. Or adding a new field to an IRS tax form in the middle of filing season. As an isolated act, adding the field isn't hard. What's hard is the notion of adding it to the tax form via a system modification when that

system is going through an intense time, with a lot of moving parts involved, and where a wrong move could actually screw the whole system up.

An alternative to changing the core plan data submission/management process and systems (i.e., modifying the carrier plan data templates, HIOS, the QHP database, and rating engine logic) would be to set up a database of logos outside this core data management process and have the FFM system, when rendering a given insurance product, pull from both the QHP database plus the logo database. This is a terrible idea technically, would be prone to error, and still creates the issue of mucking with the jet engine while it's in flight.

The right way to add logos to the FFM would be to modify the core plan data submission/management process and systems to include logos as part of the carrier plan/product template and be able to process logos all the way through. This is not doable for Oct 1 without introducing significant operational risk to the go-live, as discussed above. We suggest considering it as part of a future release, post October 1 -- understanding that it will have to compete with a lot of priorities. The reasonable thing to do would be to target making this modification in time for the next cycle of plan bids, in 2014.

From: Fontenot, Keith J.
Sent: Friday, March 08, 2013 8:19 PM
To: VanRoekeel, Steven; Park, Todd; 'donna.roy@ [DHS]'; 'robert.carey@ [DoD]'; 'Frank.Baitman@ [HHS]'; 'Marilyn.Tavener@ [CMS]'; 'dandrews@ [Pester Corp]'; 'Beatrice.Disman@ [SSA]'; 'Debbi.Russell@ [SSA]'; 'Terence.V.Milholland@ [IRS]'; 'Alan.Constantian@ [VA]'; Schlosser, Lisa; Rice, Dave; Overstreet, Tyler J.; Ple-Plakon, Alisa; Marín, Kathryn; Reczek, Jeff; Tran-Lam, Minh-Hai; Reilly, Thomas M.; 'Paula.Friedman@ [DoD]'; 'Mary.Justis@ [DoD]'; 'Monique.outerbridge@ [CMS]'; 'tony.trenkle@ [CMS]'; 'henry.chao@ [CMS]'; 'Sarah.H.Ingram@ [IRS]'; 'james.kerr@ [CMS]'; 'Silvana.G.Garza@ [IRS]'; 'Michelle.Snyder@ [CMS]'; 'Christi.Dant@ [HHS]'; 'rebecca.gwilt@ [CMS]'; 'thomas.schankweiler@ [CMS]'; 'Timothy.Monteone@ [HHS]'; 'Maribel.Franey@ [CMS]'; 'Selena.Hunn@ [IRS]'; Williams, Ross; 'Debra.McKeldin1@ [CMS]'; 'Martin.L.Pippins@ [IRS]'; 'Merle.Townley@ [DFM]'; 'Bryan.Sivak@ [IRS]'; 'Catherine.E.Livingston@ [TAMU]'; Rzeczkowski, Kristin; Lynch, Laura; Graubard, Vivian; 'Danielle.Bivens@ [DHS]'; 'EVELINE.RESURRECCION.ctr@ [DoD]'; 'Elizabeth.Callaghan@ [HHS]'; 'Alicia.Cavanaugh@ [CMS]'; 'cathy.keating@ [SSA]'; 'donna.landis@ [SSA]'; 'Ronald.Thompson@ [HHS]'; 'sandra.kraft@ [CMS]'; 'staccardo.t.washington@ [IRS]'; 'tim.m.may@ [SSA]'; 'Bennett.blodgett@ [CMS]'; 'susan.mcnelly@ [OPM]'; 'Gita.Uppal@ [VA]'; 'David.Bowen@ [DoD]'; 'joanna.walsh@ [IRS]'; 'jadyn.landis@ [SSA]'; 'carla.clark@ [DoD]'; 'Wanda.J.Brown2@ [IRS]

Cc: Rzeczkowski, Kristin
Subject: Restructuring of the Affordable Care Act Information Technology Exchange Steering Committee

Steve, Todd, and I established the executive IT steering committee (ITSC) to bring your agencies together to facilitate progress on key issues of concern and help resolve roadblocks associated with Exchange IT implementation. Now that States have made final decisions to use a Federal, Partnership, or State-based Exchange, we need to optimize use of your time and make the ITSC and workgroup meetings as efficient as possible. To this end, we will restructure ITSC by implementing the following changes immediately:

Meeting Schedules

- There will be monthly ITSC meetings, with option to cancel if necessary.
- Agency membership will not change, but meeting attendance will only be mandatory for agencies that are involved in selected agenda topics.
- Ad hoc meetings with key agencies on specific issues will continue.
- IT Exchanges workgroup and sub-workgroup meetings and activities will continue.

Streamlined Coordination

- The Centers for Medicare and Medicaid Services (CMS) will provide an agenda and relevant background materials 24 hours in advance of each ITSC meeting, which will serve to update the committee on progress, scheduling, and bring any obstacles, sources of delay, or similar issues, as well as recommendations, to the committee's attention.

- ITSC meeting agendas will focus on individual major Exchange functions (e.g., Financial Management, Eligibility and Enrollment, etc.) and how each relevant agency is preparing to "go live." Topics discussed will include issues in need of resolution or specific updates requested by ITSC chairs.
- Pre and post meeting materials should be prepared only if necessary or when materials are specifically requested by the ITSC chairs.
- The primary responsibility of the Executive Secretariat, led by the Department of Health and Human Services (HHS), is to support the workgroups and sub-workgroups.
- Participating agencies will identify one point of contact to escalate issues to the ITSC chairs within 3 business days of issuance of this memorandum.
 - o Agencies should attempt to resolve issues prior to escalation to ITSC chairs.
 - o ITSC chairs established a distribution list for direct escalation. Emails should be sent directly to me, Steve, and Todd with cc: to Minh-Hai Tran-Lam (██████████), Jeff Rezek (██████████), and Alisa Ple-Plakon (██████████) to ensure expedited responses.

We anticipate that these changes will facilitate efficient and effective ITSC meetings in the future. Thank you for your dedication to ensuring the successful implementation of the Health Insurance Marketplace to improve access to quality affordable health care coverage across the nation.

Keith

ACA IT Exchange Steering Committee Meeting Minutes
November 29, 2012

Meeting Minutes

Subject	ACA IT Exchange Steering Committee	Date	January 11, 2013
Facilitator	Ron Thompson, HHS PMO	Time	9:00 AM – 10:00 AM
Location	WHCC – Eisenhower Room	Agenda	Selena Hunn, HHS PMO & Ashley Hill, HHS PMO
Steering Committee Members Present	<p>Steering Committee Co-Chairs, Executive Office of the President:</p> <ul style="list-style-type: none"> • Keith Fontenot • Steven VanRoekel • Todd Park <p>Steering Committee Members:</p> <ul style="list-style-type: none"> • Alan Constantian, VA • Beatrice Disman, SSA • Kelly Croft, SSA • Robert Carey, DOD • Frank Baitman, HHS • Tony Trenkle, CMS 		
Additional Attendees	<p>CMS: Henry Chao, Maribel Franey, Monique Outerbridge, Jim Kerr, Tom Schankweiler, Rebecca Gwilt, Aaron Wesolowski</p> <p>DHS: Dorina Roy</p> <p>DoD: Mary Kay Justis, Capt. Margaret Beaubien</p> <p>HHS: Ron Thompson, Christi Dant, Wayne Dustin, Selena Hunn, Ashley Hill, Claudia Williams, Bryan Sivak</p> <p>IRS: Marty Pippins, Wanda Brown, Gina Garza, Cathy Livingston</p> <p>OMB: Katie Martin, Minh-Hair Tran-Lam, Jeffrey Roczek, Ailsa Ple-Plakon, David Rice, Tyler Overstreet</p> <p>OPM: Merle Townley</p> <p>SSA: Tim May</p> <p>VA: Gita Uppal</p>		

Key Points Discussed		
No.	Topic	Highlights
1	Opening Remarks and Roll Call	<p>OMB has been working at accomplishing the requests from the previous SC meeting.</p> <p>The meeting's agenda includes: key updates, Security and Privacy updates from Tim May and Rebecca Gwilt, Operations and Oversight updates from Wanda Brown and Monique Outerbridge, a CMS timeline update from Maribel Franey, and identification of</p>

Key Points Discussed		
No.	Topic	Highlights
2	Workgroup Updates	<p>dependencies from consent.</p> <p>Marilyn Taverner has been engaged in the consent resolution conversations.</p> <ul style="list-style-type: none"> Details cannot be flushed out until these conversations are complete. CMS has been ordered to await the completion of these discussions before determining the necessary changes to the baseline schedule. <p>Todd Park has been engaged in discussion on NIST Level 2 inter-mechanics.</p> <ul style="list-style-type: none"> CMS is moving forward with following this process, which represents SSA's understanding, as well. SSA is interested in understanding the downstream impact on the overall integrated testing, as well as the timeline. <p>Scheduling</p> <ul style="list-style-type: none"> Highest risk to implementation associated with waiting the high-level decision, as opposed to building for the worst case scenario: <ul style="list-style-type: none"> Broad risk: Schedule and implementation risks would be the largest concerns. The schedule presents a risk of a 2-4 week delay. The team must agree that the schedule risk is a priority and must find ways to retrieve the lost time from other areas. It is unclear as to whom the Secretary is in discussion with or what the status of the discussion is. Teams thought there would be simultaneous development between the legal issue and the IT build as the higher level issues were being addressed. The interagency team is not in full agreement on this issue. David Black would like the teams to continue making technology progress. <p>Clarification: Identification Proofing vs. Consent</p> <ul style="list-style-type: none"> Consent is a legal issue, whereas, identity proofing is a solution and process that needs to be established. SSA is relying on the Privacy Act for legal authority on ID proofing as there is none provided in the Act. <ul style="list-style-type: none"> Legal team is currently working this issue. Identity proofing would be built in as a process for verifying an individual's identity. Previous decision to use two IRS challenge questions at the threshold has been reconsidered and is currently being discussed. Suggestion: A smaller group of key individuals may need to reconvene on this topic in 3-4 weeks including Marilyn because of her involvement with the scheduling. <p>Integrated Project Plan</p> <ul style="list-style-type: none"> The IPP needs to be addressed before focusing on the schedule

Key Points Discussed		
No.	Topic	Highlights
		<ul style="list-style-type: none"> • There is some ambiguity between teams on day to day IPP control • The majority of the current schedule belongs to CMS (80-90%) making it seem as if the majority of tasks belong to CMS <ul style="list-style-type: none"> ○ CMS is unclear if other agencies are on the schedule and if there is an integrated process. ○ CMS would like other agencies to be involved to the point that we can see the integration, focusing on agency involvement in the design, development, and/or testing phases. ○ Unless everyone is operating off of the CMS schedule, scheduling should be dependent on the IPP. Currently not all are operating from the CMS schedule. <p>Eligibility and Enrollment:</p> <ul style="list-style-type: none"> • Issuers have to submit QHPs on March 28, 2013 <ul style="list-style-type: none"> ○ Goal: OMB's submission is to bring in two or more multi-state plans per state with an increase in every state over time. ○ The objective was to contract and lease to develop software that will allow multi-state plans to present their different qualifications, allowing OMB to assess and submit information to the system. ○ Phases of the application: <ul style="list-style-type: none"> ▪ Phase 1: Feb 1 – Applications due; ▪ Phase 2: March 15 – Review begins; ▪ Phase 3: May/June – Creation of answer set (a difficult problem, information goes to FFE via HIOS); ▪ Phase 4: Not addressed. • Best course of action: <ul style="list-style-type: none"> ○ The first concern with scheduling is meeting the March 28, 2013 date, the other issues may be consent etc., but March 28th is fast approaching and has not been talked about in the meetings yet. ○ The agencies responsible for build and process components that impact the March 28th date should come together, they can inform OMB of what is going on. ○ Need to determine what the key dates are, then build progress and identify roadblocks for each involved agency.
3	OMB Concerns	<p>Use of Steering Committee Meetings</p> <ul style="list-style-type: none"> • OMB would like unresolved interagency issues to be elevated during these meetings <ul style="list-style-type: none"> ○ SC meetings are not intended as a venue for reporting standard updates but rather a place to seek help on interagency roadblocks ○ The SC meetings should help maximize the productivity of delivery. ○ The meeting schedule can/should be utilized according to necessity.

Key Points Discussed		
No.	Topic	Highlights
		<ul style="list-style-type: none"> ▪ Only hold meetings when need be, otherwise it is permissible to cancel the standing appointment. ▪ OMB wants to know from the interagency teams how OMB can do a better job of helping solve relevant issues and meeting with the team. <ul style="list-style-type: none"> ▪ The Interagency team would like to come back to OMB with a proposal on the best way to raise interagency issues that need their help in order to reach benchmarks.

Action Items from 1/11/13			
No.	Action Item(s)	Owner	Target Date
1	Produce a document for SC detailing how they would benefit from OMB assistance and meeting in the future.	Interagency team	2-3 weeks

DRAFT

461

To: Coutts, Todd (CMS/OIS) (Todd.Coutts1@cms.hhs.gov|Todd.Coutts1@cms.hhs.gov)
Cc: Calera, Mark (CGI Federal)|Mark.Calera@cgi.com; Weiss, Paul (CGI Federal)|Paul.Weiss@cgi.com
From: Manambedu, Lakshmi (CGI Federal)
Sent: Fri 7/12/2013 6:11:47 PM
Subject: RE: Need a write up for Todd
[Day One Capabilities - Priority and Risk - 20130712.docx](#)

Hi Todd,

Attached is what I have for E&E. You may be able to extract the major ones from this.

In terms of other major milestones between Oct 1 and Jan 2014 are:

- Enrollment Reconciliation – December 2013
- Exemptions Applications – December 2013
- Payment to Issuers – 3rd week of January 2014

Thank you

Lakshmi Manambedu | Vice President, CGI Federal | Mobile: [REDACTED] www.cgi.com

From: Chao, Henry (CMS/OIS) [mailto:henry.chao@cms.hhs.gov]
Sent: Friday, July 12, 2013 12:58 PM
To: Manambedu, Lakshmi (CGI Federal); Karlton Kim (kkim@cms.hhs.gov); Donohoe, Paul X. (CMS/OIS);
Coutts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Cc: Oh, Mark U. (CMS/OIS); Berkeley, Katrina (CMS/OIS); Coutts, Todd (CMS/OIS); Rhones, Rhonda D.
(CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: Need a write up for Todd
Importance: High

This is for sources material for Todd Park to pick nuggets from in his prep for briefing POTUS next week.

So the write-up which are sentence(s) in bullet format needs to cover:

- [REDACTED] The A-Z of testing by partner (Issuer, # of Issuers, State programs, types of Marketplace, approach (waves, harness, DE, 834/enrollment, etc.), and high level schedule.
- [REDACTED] Overall list of key activities to be accomplished and risks for Day one (remaining 80 days) and Day ones for other major lifts prior to Day one of the benefit and the start of the benefit.

Please use material we have already like the deck that we used for SVR and updated another version for Marilyn/OL a few days ago.

Remember that bullets should not be written to be used to create more questions.

Rhonda and Todd—please collect, format, and send to me by COB today.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services

[REDACTED]
[REDACTED]

Message

From: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent: 9/3/2013 11:06:25 PM
To: Trenkle, Tony (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]; Baitman, Frank (OS/ASA/OCIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Frank.Baitman.OS]; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]
Subject: Fw: Cybersecurity points

Tony, Frank, Michelle, thoughts on Ed joining our 10 am call tomorrow, and then talking with him afterwards briefly? One point to discuss with him is Frank's very good point that we need to walk a fine line publicly -- showing we take the risks seriously but also not baiting hackers into attacking.

Also: it was part of the outline for tomorrow's call, but just wanted to follow up on if we can get some external validators to be references with respect to CMS's general cyberdefenses and approach to cybersecurity -- again, in the context of the walking the fine line above....

Thanks so much,
 Todd

----- Original Message -----

From: Siskel, Edward
Sent: Tuesday, September 03, 2013 05:14 PM
To: Park, Todd
Subject: FW: Cybersecurity points

-----Original Message-----

From: Jennings, Christopher
Sent: Tuesday, September 03, 2013 4:33 PM
To: Siskel, Edward; McGuinness, Tara; Lambrew, Jeanne; Park, Todd
Cc: Jones, Isabel; 'aryana.khalid@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov'; 'tony.trenkle@cms.hhs.gov'; 'frank.baitman@hhs.gov'; Graubard, Vivian
Subject: Re: Cybersecurity points

Todd and gang;

Thanks all.

Chris

----- Original Message -----

From: Jennings, Christopher
Sent: Tuesday, September 03, 2013 07:12 AM
To: Park, Todd; Siskel, Edward
Cc: Lambrew, Jeanne; Jones, Isabel; 'aryana.khalid@cms.hhs.gov' <aryana.khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: Re: Cybersecurity points

Thank you Todd and all on this email. Very helpful and greatly appreciated.

Thanks to all

for this background and, more importantly, your great work to protect us from cyber attacks/security threats.

Chris

----- Original Message -----

From: Park, Todd

Sent: Tuesday, September 03, 2013 01:38 AM

To: Jennings, Christopher

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris, here are an expanded/updated set of bullet points from Frank and Tony:

- Like all publicly facing Internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state of the art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff: when the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.
- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.
- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US-CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----

From: Jennings, Christopher

Sent: Monday, September 02, 2013 02:43 PM

To: Park, Todd

Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

HHS-0106447

-----Original Message-----

From: Park, Todd
 Sent: Monday, September 02, 2013 2:19 PM
 To: Jennings, Christopher
 Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov';
 'tony.trenkle@cms.hhs.gov'; 'frank.baitman@hhs.gov'; Graubard, Vivian
 Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people -- they are tracking folks down today and will seek to get you additional info by tonight.... BUT if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
 Todd

----- Original Message -----

From: Jennings, Christopher
 Sent: Monday, September 02, 2013 12:28 PM
 To: Park, Todd
 Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>;
 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov'
 <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
 Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder [REDACTED]. We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----

From: Park, Todd
 Sent: Monday, September 02, 2013 12:02 PM
 To: Jennings, Christopher
 Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov';
 'tony.trenkle@cms.hhs.gov'; 'frank.baitman@hhs.gov'; Graubard, Vivian
 Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for you [REDACTED]. The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also

466

working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

-- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,
Todd

HHS-0106449

-- Application of this information security program to the Marketplace provides strong, sound safeguards for consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage.

From: Park, Todd
Sent: Tuesday, September 17, 2013 9:54 PM
To: Santillo, Jessica; 'tony.trenkle@cms.hhs.gov'
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman@hhs.gov'; 'Brian.Cook@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov'
Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Tony/Frank, an update -- it looks like the background call tomorrow is with WH folks only, with detailed inquiries to be referred to agencies.

So; while I'd love for you to hold the time on your calendars (just in case), as of this moment, you don't have to get on the call :)

I've let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can talk to it at a general level only -- she thinks that will be OK on the call tomorrow, with detailed questions to be referred to agencies.

Just to triple check this, I will be sending around talking points tonight which (combined with Marilyn's Hub letter) basically represent what I'm prepared to say tomorrow. Would very much appreciate your vetting of these.

And in the event that, after reviewing my talking points, Jessica feels like we need more on the call, we may ask you to attend the call after all :)

So while you are off the hook for now, please do hold the call time, just in case!

Thanks so much, and please stay tuned for talking points to vet, coming later tonight.

Todd

From: Park, Todd
Sent: Tuesday, September 17, 2013 07:39 PM
To: Santillo, Jessica; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; 'Brian.Cook@cms.hhs.gov' <Brian.Cook@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>
Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

OK, will draft talking points and send around later tonight. And Tony/Frank, please confirm if you can join me on this background call -- again, only to participate in the cybersecurity portion :) Would really appreciate your help :)

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 07:37 PM
To: Park, Todd; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; 'Brian.Cook@cms.hhs.gov'

<Brian.Cook@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Thanks Todd – if your team could draft the cyber talking points, that would be very helpful. Thanks so much.

We are still working on finalizing the paper but will share those with everyone as soon as they are ready.

From: Park, Todd
Sent: Tuesday, September 17, 2013 7:22 PM
To: Santillo, Jessica; 'tony.trenkle@cms.hhs.gov'
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman@hhs.gov'; 'Brian.Cook@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov'
Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Thanks, Jessica. Tony and Frank, can you join via phone? You'll only be asked to help with the cybersecurity part of the call :) I am more than happy to deliver the primary talking points, which will focus principally on Marilyn's letter regarding Hub cybersecurity + the general points the three of us hammered out a while back.

Jessica, are you putting together talking points for us, or would you like me to take a crack at them?

Thanks,
Todd

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 07:13 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS) <tony.trenkle@cms.hhs.gov>
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO) <Frank.Baitman@hhs.gov>; Cook, Brian T. (CMS/OC) <Brian.Cook@cms.hhs.gov>; Snyder, Michelle (CMS/OA) <Michelle.Snyder@cms.hhs.gov>
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Todd – happy to have Tony and Frank join us for the cyber security portion.

On your first question – the call is on background according to “White House officials.”

Thanks very much for making this work on such short notice. We will hold the call in EEOB 207. I will send around a calendar invite.

Thank you again,
Jessica

From: Park, Todd
Sent: Tuesday, September 17, 2013 6:14 PM
To: Trenkle, Tony (CMS/OIS); Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Tony, the part of the call where you, Frank, and I would be participating would focus exclusively on cybersecurity...

Jessica, thoughts?

From: Trenkle, Tony (CMS/OIS) [<mailto:tony.trenkle@cms.hhs.gov>]
Sent: Tuesday, September 17, 2013 5:08 PM
To: Park, Todd; Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Todd,

I am not really comfortable about participating on this call, even on background. It is getting into areas that I have not been involved in (privacy and fraud prevention efforts).

Tony

From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Tuesday, September 17, 2013 4:43 PM
To: Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Trenkle, Tony (CMS/OIS); Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Jessica, I am signed up to help with the call! Looping Tony, Frank, and Brian. Two questions:

1. <!--[if !supportLists]--><!--[endif]-->Is the call on background, or on the record?
2. <!--[if !supportLists]--><!--[endif]-->Can Tony Trenkle and Frank Baitman join me on the call? They are the folks who know the details, and it would be super-helpful for them to be on.

Thanks!

Todd

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 2:10 PM
To: Park, Todd
Cc: Jones, Isabel; Mielke, Dawn M.
Subject: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Todd –



From: Park, Todd
Sent: Monday, January 07, 2013 11:20 PM
To: 'Bryan.Sivak@HHS'
Subject: Re: Fwd: Consent issue

Yes, let's cover when we chat tomorrow. And the 9 am meeting is the ACA Steering Committee mtg (WH/interagency) that you're now supposed to be invited to.... I'll check with Minh -Hai to make sure you're invited!!

From: Sivak, Bryan (HHS/IOS) <[REDACTED]>
Sent: Monday, January 07, 2013 09:34 PM
To: Park, Todd
Subject: Fwd: Consent issue

Two things: first, check the thread (keep this between us). We should probably talk about this.

Second, do you know anything about a meeting Friday morning? It's not on my calendar.

Begin forwarded message:

From: "Baitman, Frank (OS/ASA/OCIO)" <[REDACTED]>
Date: January 7, 2013, 21:06:31 EST
To: "Sivak, Bryan (HHS/IOS)" <[REDACTED]>
Subject: Re: Consent issue

There's an ACA meeting on Friday at 9am. I'd thought you were put on the invite list. I'll look into it.

I'm told that SSA is preparing some position papers that seem to indicate there are problems with consent through the Privacy Act. Seems like you're hearing something else? So, are SSA and IRS on board with the resolution?

- F

Frank Baitman
Sent from my iPad
please excuse my typos!

On Jan 7, 2013, at 7:40 PM, "Sivak, Bryan (HHS/IOS)" <[REDACTED]> wrote:

I think we pretty much have it resolved although I'll know more by mid week.

I don't think it will really matter, but what are the "additional impediments?"

471

Also...what meeting on Friday? I don't have anything on my calendar.

On Jan 7, 2013, at 19:34, "Baitman, Frank (OS/ASA/OCIO)"
<[REDACTED]> wrote:

Bryan, just wondering where this stands now? Are you working it?

I'm told that CMS has gotten quiet on this, and our folks don't know where this is going.

From an SSA perspective, it sounds like there might be some additional impediments from their end.

Since we have the WH meeting on Friday, I'd like to understand any challenges in advance.

Thanks,
- Frank

