

THE THREAT TO AMERICANS' PERSONAL INFORMATION: A LOOK INTO THE SECURITY AND RELIABILITY OF THE HEALTH EXCHANGE DATA HUB

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 11, 2013

Serial No. 113-33

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpo.gov/fdsys/>

U.S. GOVERNMENT PRINTING OFFICE

86-247 PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas	BENNIE G. THOMPSON, Mississippi
PETER T. KING, New York	LORETTA SANCHEZ, California
MIKE ROGERS, Alabama	SHEILA JACKSON LEE, Texas
PAUL C. BROUN, Georgia	YVETTE D. CLARKE, New York
CANDICE S. MILLER, Michigan, <i>Vice Chair</i>	BRIAN HIGGINS, New York
PATRICK MEEHAN, Pennsylvania	CEDRIC L. RICHMOND, Louisiana
JEFF DUNCAN, South Carolina	WILLIAM R. KEATING, Massachusetts
TOM MARINO, Pennsylvania	RON BARBER, Arizona
JASON CHAFFETZ, Utah	DONDALD M. PAYNE, JR., New Jersey
STEVEN M. PALAZZO, Mississippi	BETO O'ROURKE, Texas
LOU BARLETTA, Pennsylvania	TULSI GABBARD, Hawaii
CHRIS STEWART, Utah	FILEMON VELA, Texas
RICHARD HUDSON, North Carolina	STEVEN A. HORSFORD, Nevada
STEVE DAINES, Montana	ERIC SWALWELL, California
SUSAN W. BROOKS, Indiana	
SCOTT PERRY, Pennsylvania	
MARK SANFORD, South Carolina	

GREG HILL, *Chief of Staff*

MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*

MICHAEL S. TWINCHEK, *Chief Clerk*

I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION,
AND SECURITY TECHNOLOGIES

PATRICK MEEHAN, Pennsylvania, *Chairman*

MIKE ROGERS, Alabama	YVETTE D. CLARKE, New York
TOM MARINO, Pennsylvania	WILLIAM R. KEATING, Massachusetts
JASON CHAFFETZ, Utah	FILEMON VELA, Texas
STEVE DAINES, Montana	STEVEN A. HORSFORD, Nevada
SCOTT PERRY, Pennsylvania, <i>Vice Chair</i>	BENNIE G. THOMPSON, Mississippi (<i>ex officio</i>)
MICHAEL T. MCCAUL, Texas (<i>ex officio</i>)	

ALEX MANNING, *Subcommittee Staff Director*

DENNIS TERRY, *Subcommittee Clerk*

CONTENTS

	Page
STATEMENTS	
The Honorable Patrick Meehan, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Emergency Preparedness, Response, and Communications	1
The Honorable Yvette D. Clarke, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Emergency Preparedness, Response, and Communications:	
Oral Statement	3
Prepared Statement	6
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement	7
WITNESSES	
Mr. Michael J. Astrue, Former Social Security Commissioner, Former U.S. Department of Health and Human Services General Counsel:	
Oral Statement	9
Prepared Statement	11
Mr. Stephen T. Parente, Ph.D., Minnesota Insurance Industry Chair of Health Finance, Director, Medical Industry Leadership Institute, Professor, Department of Finance, Carlson School of Management, University of Minnesota:	
Oral Statement	13
Prepared Statement	15
Ms. Kay Daly, Assistant Inspector General, Audit Services, U.S. Department of Health and Human Services:	
Oral Statement	16
Prepared Statement	17
Mr. Matt Salo, Executive Director, National Association of Medicaid Directors:	
Oral Statement	21
Prepared Statement	23
FOR THE RECORD	
The Honorable Yvette D. Clarke, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Emergency Preparedness, Response, and Communications:	
Letter	5

THE THREAT TO AMERICANS' PERSONAL INFORMATION: A LOOK INTO THE SECURITY AND RELIABILITY OF THE HEALTH EXCHANGE DATA HUB

Wednesday, September 11, 2013

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE
PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 2:02 p.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Rogers, Marino, Perry, Clarke, Vela, and Horsford.

Also present: Representative Jackson Lee.

Mr. MEEHAN. The Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order.

The subcommittee is meeting today to examine the security and reliability of the Health Exchange Data Hub and the existence of any threat to Americans' personal information.

Before beginning my opening statement, I think it is only appropriate on a day like today that we take a moment and join in a moment of silence, remembrance of the victims of September 11 as we recognize the twelfth anniversary of that terrible tragedy.

I thank you.

I now recognize myself for an opening statement.

Today's hearing, "A Threat to Americans' Personal Information: A Look into the Security and Reliability of the Health Exchange Data Hub" is the second hearing on this issue in less than 2 months by this committee or associated with this committee.

The Federal Data Services Hub was established under the rulemaking for the Patient Protection and Affordable Care Act. Its purpose is to be the one-stop shop to connect applicants to the Affordable Care Act exchanges.

The hub will connect to multiple Federal agencies including the Social Security Administration to verify an applicant's Social Security number, the IRS, to verify income and really not just for an applicant, but for an applicant's spouse and children and others.

The Department of Homeland Security to verify citizenship and immigration status as well as other Federal agencies to determine an applicant's eligibility for Federal health insurance subsidies, the

key aspect of it to be the ability to articulate the qualification, not just for subsidies but amount of subsidies.

Personally identifiable information for any applicant and their families will pass through the data hub from these various agencies. In fact, over 20 million Americans are expected to enter the exchange over the next 5 years, and I know we will hear testimony about what the scope of this exchange is expected to be.

This information will include an applicant's name, address, date of birth, Social Security number, household income, health status including whether an applicant is pregnant or has a disability, and will be stored in the exchange system of records for up to 10 years, stored in the system for up to 10 years.

The Government Accountability Office in a June 2, 2013 report called the hub, "a complex undertaking involving the coordinated actions of multiple Federal, State, and private stakeholders." The report concluded that, "a timely and smooth implementation by October 13, 2013 cannot yet be determined."

In July, this subcommittee convened a joint hearing with the House Oversight and Government Reform Subcommittee. We heard directly from Centers for Medicare and Medicaid Services, Director Marilyn Tavenner, and acting commissioner of the IRS, Daniel Werfel, among others on the implementation of the hub.

My personal take-away from that hearing is that CMS was not ready to embark on this giant responsibility. Since our hearing, the Health and Human Services inspector general conducted a report on the implementation of the hub from a security perspective.

The IG report stated that the several critical tasks remained to be completed in a short period of time. That is why we are here today, to examine CMS' progress in securing America's personal information.

I am thankful to the inspector general who sent a representative to participate in today's hearing. As we sit just 20 days removed from the exchanges and the data hub, going live on October 1, I have grave concerns from a cybersecurity standpoint.

We have assembled a panel of witnesses uniquely qualified in commenting on the scope and readiness of the mounting task at hand. I thank them for participating, and I look forward to hearing their testimonies.

Let me conclude my comments by saying that this is not a hearing that goes into the policy implications behind the Affordable Care Act. It is not our purpose here today to try to raise that issue.

But we are a committee that is focused and focused importantly on the security of American citizens, and one of the highest issues we currently see is an appreciation for personal privacy and private identifying information and what the misuse of that information cannot just mean directly to a person but to a person who then has to go about trying to fix that in their lives.

In the best of times, we have seen dramatic growth in those who have used and developed new and innovative ways to steal that information to use it in the markets in a variety of different capacities.

So as we have dealt with increasing sophistication in those who would try to steal them and manipulate this information, we also recognize that we are in a unique time as well.

A time in which cyber information is not just there to be manipulated or used or stolen by those if it is not appropriately secure, but we face a time in which there are very sophisticated actors, including state actors who may wish to do us harm.

A database that it is the core of one of the central expenditures of American resources can certainly, foreseeably be a target. The extent to which we are ready not just for the kinds of challenges that are facing security databases in the normal course of business but the preparation readiness to stand up to what may be a sophisticated attack and one that seeks to do us damage are all relevant considerations for us at this important point.

These are some of the issues I want to ask about the readiness before we get ready to go, and I appreciate those of you who are here today who are ready to testify on your opinions and knowledge with regard to the readiness of this database.

Now the Chairman now recognizes the Ranking Minority Member of the subcommittee, the gentlelady from New York, Ms. Clarke, for any statement that she may have.

Ms. CLARKE. I thank you, Mr. Chairman, for holding a second hearing on one of the most important features of the Affordable Care Act, and I welcome our witnesses here today.

When President Obama signed the Affordable Care Act in the East Room of the White House on March 23, 2010, the Federal Government started planning to operate health care insurance market places, also called exchanges, and assist States that opted to run their own marketplaces.

All of this involves developing a complex computer web-based service that would allow millions of Americans access to affordable health care in the most efficient and safe way possible.

This is a large undertaking and involves a complicated inter-agency IT and web-based software effort commonly known as the Federal Data Services Hub based at the Department of Health and Human Services Center for Medicare, Medicaid Services, or CMS.

What is important about this effort is that we must create, collect, and use or disclose personal information of millions of our citizens in a responsible and confidential way.

The health care marketplaces must establish and implement cyber and personal information protection standards that are consistent with specific principles outlined in our current health care law.

Those principles which are comparable to the ones upon which the HIPAA, the Health Insurance Portability and Accountability Act, provide and they include No. 1, providing a right of access to one's personally identifying information commonly referred to as PII, a right to have erroneous information corrected, and No. 3, providing accountability through appropriate monitoring and reporting of information breaches.

Exchanges must also establish and implement reasonable operational, technical, administrative, and physical safeguards to ensure the confidentiality, integrity, and availability of PII and to prevent unauthorized or inappropriate access, use, or disclosure of PII.

In addition, health exchanges must monitor, periodically access, and update their security controls and must develop and use secure electronic interfaces when sharing PII electronically.

CMS has completed its technical design and build of Federal Data Services Hub and has established an inter-agency security framework as well as the protocols for connectivity.

Importantly, in a letter to Ranking Member Thompson this morning, HHS has revealed that as of Friday, September 6, they had taken the necessary steps to obtain security authorization for the data hub and the CMS chief information officer has assigned to the security authorization.

This is an important milestone and it shows that CMS will be ready to operate the hub securely on October 1.

This will provide a common, secure connection for marketplaces to seek information from Federal databases necessary to verify eligibility, excuse me, for the millions of Americans who can begin to shop for quality, affordable health care coverage in just a few weeks.

The hub has several layers of protection to mitigate information security risks. For example, marketplace systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action.

Let us remember, it is simple. The Data Services Hub will transfer data and be used to verify applicant information data for eligibility. The Data Services Hub is not a database. It will not function as a database. It will not contain health care records.

The hub will send queries and responses among given marketplaces and data services to determine eligibility. The Data Services Hub will not determine consumer eligibility nor will it determine which health plans are available in the marketplaces.

CMS and its vendors have told us and testified before this subcommittee and Energy and Commerce subcommittees that delivery milestones for the Data Services Hub completion are being met on time and they expect that the Data Services Hub will be ready as planned by October 1.

I am looking forward to the testimony of the HHS Office of the Inspector General to learn more about their important role in the implementation of the Federal data hub.

Also, we are going to hear testimony today from the director of the State Medicaid Directors Association whose members have been working on this effort from the ground up.

I am eager to learn about the massive efforts of that State and the Federal Centers for Medicaid and Medicaid Services have made to stand up to this complex data hub. This is the kind of information we need to help us deliver health care to citizens who really need it.

Mr. Chairman, I ask for unanimous consent to submit a copy of the letter received by Ranking Member Bennie Thompson.

Mr. MEEHAN. Without objection, so ordered.

[The information follows:]

LETTER SUBMITTED BY RANKING MEMBER YVETTE D. CLARKE

Washington, DC, 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 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 comports 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 on-going 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.

Ms. CLARKE. Thank you, Mr. Chairman, and I yield back.
[The statement of Ranking Member Clarke follows:]

STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

SEPTEMBER 11, 2013

Thank you Mr. Chairman for holding a second hearing on one of the most important features of the Affordable Care Act.

When President Obama signed the Affordable Care Act in the East Room of the White House on March 23, 2010, the Federal Government started planning to operate health care insurance marketplaces, also called exchanges, and assist States that opted to run their own marketplaces.

All of this involves developing a complex computer web-based service that would allow millions of Americans access to affordable health care, in the most efficient and safe way possible.

This is a large undertaking, and involves a complicated inter-agency IT and web-based software effort, commonly known as a "Federal Data Services Hub" based at The Department of Health and Human Services, Center for Medicare and Medicaid Services, or CMS.

What is important about this effort is that we must create, collect, and use or disclose personal information of millions of our citizens in a responsible and confidential way.

The health care marketplaces must establish and implement cyber and personal information protection standards that are consistent with specific principles outlined in our current health care law.

Those principles, which are comparable to the ones upon which the HIPAA, the Health Insurance Portability and Accountability Act provide, and they include:

- Providing a right of access to one's Personally Identifying Information, commonly referred to as PII;
- A right to have erroneous information corrected;
- And providing accountability through appropriate monitoring and reporting of information breaches.

Exchanges must also establish and implement reasonable operational, technical, administrative, and physical safeguards to ensure the confidentiality, integrity, and availability of PII, and to prevent unauthorized or inappropriate access, use, or disclosure of PII.

In addition, Health Exchanges must monitor, periodically access, and update their security controls, and must develop and use secure electronic interfaces when sharing PII electronically.

CMS has completed its technical design, and build of Federal Data Services Hub and has established an interagency security framework as well as the protocols for connectivity.

Importantly, in a letter to Ranking Member Thompson this morning, HHS has revealed that as of Friday, September 6, they had taken the necessary steps to obtain security authorization for the data hub, and the CMS Chief Information Officer has signed the security authorization. This is an important milestone, and it shows that CMS will be ready to operate the hub securely on October 1.

This will provide a common, secure connection for Marketplaces to seek information from Federal databases necessary to verify eligibility for the millions of Americans can begin to shop for quality, affordable health coverage in just a few weeks.

The hub has several layers of protection to mitigate information security risk. For example, Marketplace systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action.

Let us remember, it's simple . . . the Data Services Hub will transfer data and be used to verify applicant information data for eligibility. The Data Services Hub is NOT a database, it will not function as a database, and it will not contain health care records.

The hub will send queries and responses among given marketplaces and data sources to determine eligibility. The Data Services Hub will not determine consumer eligibility, nor will it determine which health plans are available in the marketplaces.

CMS and its vendors have told us, and testified before this subcommittee and Energy and Commerce subcommittees, that delivery milestones for the Data Services Hub completion are being met on time, and they expect the Data Services Hub will be ready as planned by October 1.

I am looking forward to the testimony of the HHS Office of Inspector General to learn more about their important role in the implementation of the Federal Data Hub.

Also, we are going to hear testimony today from the director of the State Medicaid Directors Association, whose members have been working on this effort from the ground up.

I am eager to learn about the massive efforts that States, and the Federal Centers for Medicare and Medicaid Services, have made to stand up this complex data hub.

This is the kind of information we need to help us deliver health care to citizens who really need it.

Mr. Chairman, I yield back.

Mr. MEEHAN. Okay. I thank the gentlelady.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 11, 2013

Thank you, Mr. Chairman, for holding a second hearing on one of the most important features of the Affordable Care Act. I also want to thank the witnesses for appearing here today.

On March 23, 2010, President Obama signed the Affordable Care Act into law. I should note that today, the Majority will bring their 41st vote to undermine and repeal the Affordable Care Act to the Floor of the House. The ACA requires the development of a computer-based service that will allow millions of Americans the ability to purchase affordable health care policies for their families, in the most efficient and safest way possible. This undertaking requires the development of a "Federal Data Services Hub."

My colleagues on the other side of the aisle have used the development of this hub to promote uncertainty and fear about the ability of these computer systems to keep the personal and health information of millions of Americans safe and secure. I appreciate their concern. It seems that last year, a poll conducted by the National Foundation for Credit Counseling found that 64% of Americans fear identity theft. Given the widespread fear of identity theft, the American public should have the facts on whether there is any danger in personal and health information leaking out or being hacked from this system.

This kind of assurance is extremely important if we want millions of people who do not have health care to feel that they can trust this system and use it to get the care they need and the policies they can afford. We all know that sowing fear in a new system is one way to discourage participation and drive down enrollment figures. I am sure no one would want that outcome. So here are the facts that people need to know to have confidence in this system:

- (1) The use of computers to obtain, verify, and transmit information in Government programs is nothing new;
- (2) The information contained on your driver's license and Social Security card and any other piece of Government-issued identification you have is housed somewhere on a Government database;

(3) The Federal Government and the States already use and exchange personal data to determine eligibility for various programs;

(4) Leaks involving personal data by State and local governments are a rare occurrence. Information leaks involving personal data held by private companies, such as banks, credit card issuers, and retail stores, are common; and,

(5) As of Friday, September 6, 2013, HHS/CMS had taken the necessary steps to obtain a security authorization for this system.

Thus, while I appreciate the Majority's concern about the Government's ability to safeguard this information, it appears to be misplaced.

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

Mr. MEEHAN. I am going to take a moment to introduce the distinguished panel that we have before us, and we are appreciating having such a distinguished panel on this topic.

First, let me introduce Mr. Michael Astrue who formally served as the commissioner of Social Security from 2007 until January 2013 as well as the general counsel for the Department of Health and Human Services from 1989 until 1992.

As commissioner of Social Security, he focused his efforts on reducing the disability backlog and improving services to the public particularly through electronic services.

He spearheaded highly-successful new systems for fast-tracking disability claims, created National hearing centers to reduce backlogs, and expanded and overhauled the agency's suite of electronic services to make them simpler, faster, and more user-friendly.

Dr. Stephen Parente is the Minnesota Insurance Industry Professor of Health Finance and Insurance in the Carlson School of Management at the University of Minnesota. He specializes in health economics, health insurance, medical technology evaluation in health information technology.

He is acknowledged as a National expert on using administrative databases particularly Medicare and health insurer data for health policy research and has served as a consultant to several of the largest health care organizations in the country.

Ms. Kay Daly is the assistant inspector general for audit services at the United States Department of Health and Human Services.

Ms. Daly's responsibilities include overseeing the chief financial officer financial statement audits at HHS, reporting on compliance with improper payment acts, providing oversight of over 300 grant programs as ministered by HHS, and overseeing audits related to the implementation of health care reform.

Prior to joining HHS OIG, Ms. Daly worked at the Government Accountability Office for 23 years.

Finally, we are joined by Mr. Matt Salo. He is the executive director of the National Association of Medicaid Directors since February 2011.

This is a newly-formed association. It represents all 56 of the Nation's State and territorial Medicaid directors and provides them with a strong unified voice in National discussions as well as a locus for technical assistance and best practices.

Mr. Salo formally spent 12 years at the National Governors Association where he worked on the Governor's Health Care and Human Services agendas and spent 5 years prior to that as a health policy analyst working for the State Medicaid directors.

There will be full written statements of the witnesses which will appear in the record.

Now I have got to sort of make a judgment, and I see that we have a little less than 8 minutes to go on the existing vote responsibilities that we have. Having teed this very, very impressive panel up, I am sort of hesitant to see a rain delay.

So what I think I am going to recommend to our panel is that we will vote as quickly as we can, and I will make the representation that I will hustle back as quickly as I can, gavel in as soon as I get here, and I know my colleagues will do their best as well after last vote.

I think it is probably better to allow the panelists to testify in order than to start the process, break, and start again.

So with your forgiveness, so to speak, we thank you for understanding the nature of the world in which we work and we look forward upon our return to your testimony in engaging in, in, in our dialogue.

So, at the moment, the Chairman, the committee stands in recess.

Thank you.

[Recess.]

Mr. MEEHAN. The Committee and the Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will return to order.

I thank you once again for your indulgence. I know my colleagues are working their way back as quickly as possible, but we thank—we appreciate your indulgence, and now we would like to create the opportunity for you to begin your testimony.

As I have had said before, the full written statements of the witnesses will appear in the record. So I now look forward to the verbal testimony of each of our witnesses on the issue that we are here to meet with today.

So the Chairman now recognizes Mr. Astrue for his testimony. Thank you.

Mr. Astrue, yes, you may want to touch—thank you.

STATEMENT OF MICHAEL J. ASTRUE, FORMER SOCIAL SECURITY COMMISSIONER, FORMER U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES GENERAL COUNSEL

Mr. ASTRUE. Out of practice, sorry.

Chairman Meehan, Ranking Member Clarke, and Members of the subcommittee, no day is more fitting than 9/11 for us to cherish and safeguard our liberties as Americans. Thank you for inviting me here today.

I testify only as a former official. A quarter-century ago, I briefly was the White House's Privacy Act officer. I then served as general counsel of the U.S. Department of Health & Human Services and as commissioner of Social Security for Presidents Bush and Obama. As commissioner, I also served as a trustee of the Medicare Trust Fund.

Some history helps us understand why we needed to have this hearing. Infighting and paralysis marked the first year of the effort to construct the Federal health exchanges, including what is called the "data hub."

Administrator Berwick claimed that he could not find the money to build the system, and he criticized Congress for not specifically

appropriating money for it. He also criticized Secretary Sebelius for refusing to release money from the ACA discretionary fund.

Berwick pressed other agencies to pay for the exchanges, even though such payments would have violated appropriations restrictions. When development started in earnest after Berwick's departure, CMS struggled to meet its deadlines.

CMS' failures and delays have been common knowledge within the administration, yet HHS was never candid with the States about these problems as they were choosing either to build their own exchanges or to use the CMS exchanges.

From 2007–2013, I led the overhaul and expansion of the Social Security's suite of electronic services. I personally reviewed every major system before beta testing, and extensive beta testing often revealed the need for delays to make changes. We involved not only random focus groups, but also advocates for various people, such as victims of domestic violence.

We need to be vigilant about the privacy of the data stored in these types of systems, which I believe are not being adequately protected by CMS.

The defense offered by the HHS inspector general, the Center for Democracy & Technology, and others, that the CMS systems are just a "routing tool," not a repository, is either untrue or problematic.

CMS needs to store data to create forensic trails necessary to track security breaches. Failure to establish forensic trails would create a serious issue under the Federal Information Security Management Act of 2002 and would create a serious operational vulnerability.

We also need to know whether unauthorized changes of insurance could leave Americans unexpectedly uninsured. We need to know how CMS will define and respond to breaches.

I know how important that is because I suffered through the Office of Personal Management's inept response when my personal Federal financial records were breached 2 years ago. We need to know why many of the people who will deal with the public are just being hired now and being hired without background checks.

A rigorous authentication process may result in as many as 2 to 5 million people who will need to interact with CMS contractors when they fail to access the system. Is CMS ready for that workload or are they going to sacrifice service or authentication?

Greater transparency about these issues would have improved the quality of the exchanges and would have increased public confidence in the system, which is sorely lacking today.

Both SSA and the IRS formally appealed to OMB that the exchanges would violate the Privacy Act, violations which potentially carry criminal penalties.

OMB eventually denied that appeal, but in my view HHS will be violating the Privacy Act on a massive scale by allowing people to make insurance decisions for other adults without their written consent. This feature of the system may also allow domestic abusers to track down their victims.

An August 2, 2013 inspector general report revealed that the CMS schedule had slipped so badly that mandatory security findings were scheduled for the day before implementation.

Despite HHS' letter this morning, yesterday's testimony before the House Energy and Commerce Committee indicate that many States will be unready for October 1, and that CMS may be unready given that the contractors were still citing October 1 as their date of readiness.

The main reason we have so little information about the status of the exchanges is the failure of the office of the HHS inspector general. Relying only on interviews and documents, its August 2, 2013 report on the exchanges contained less than 5 pages of analysis; its total work product for this subject for the year.

Moreover, the inspector general did not inspect the beta version and meekly noted that CMS withheld security documents. He ignored the vulnerabilities in the system that transmits, largely through the so-called cloud, sensitive personal information to CMS contractors and private insurers.

He ignored the privacy issues, the security issues, and the issues associated with poorly screened and trained contractors. He did not assess usability, performance measures, governance, or contingency plans. With HHS' greatly expanded role in health care, Americans need an inspector general who is a watchdog, not a lapdog.

Congress is bitterly divided about the Affordable Care Act, but the topics for my presentation should be common ground. Whether or not you support an individual mandate, you can embrace the principle that no one should be forced to sacrifice privacy in order to comply with that mandate.

To the best of my knowledge, work on systems that would comply with the Privacy Act ended in early 2013. A system respecting the Privacy Act would probably take an additional 6 to 18 months to develop.

President Obama has delayed other parts of the Affordable Care Act. Vulnerable Americans without lobbyists deserve the same respect and deference given to the business community.

You should support a moratorium on the exchanges until HHS secrecy ends, and until we know whether uninsured Americans will be forced to pay, along with their premiums, the high price of their privacy, and the safety of their personal data.

Thank you.

[The prepared statement of Mr. Astrue follows:]

PREPARED STATEMENT OF MICHAEL J. ASTRUE

SEPTEMBER 11, 2013

Chairman Meehan, Ranking Member Clarke, and Members of the subcommittee, no day is more fitting than 9/11 for us to cherish and safeguard our liberties as Americans.

I testify today only as a former official. A quarter-century ago, I briefly was the White House's Privacy Act officer. I then served as general counsel of the U.S. Department of Health & Human Services and as commissioner of Social Security for Presidents Bush and Obama. As commissioner, I also served as a trustee of the Medicare Trust Fund.

Some history helps us understand why we needed to have this hearing. Infighting and paralysis marked the first year of the effort to construct the Federal health exchanges, including what is called the "data hub." Administrator Berwick claimed that he could not find the money to build the system, and he criticized Congress for not specifically appropriating money for it. He also criticized Secretary Sebelius for refusing to release money from the ACA discretionary fund.

Berwick pressed other agencies to pay for the exchange, even though such payments would violate appropriations restrictions. When development started in ear-

nest after Berwick's departure, CMS struggled to meet its deadline. CMS's failures and delays have been common knowledge within the administration, yet HHS was never candid with States as they were choosing either to build their own exchanges or to use the CMS exchanges.

From 2007–2013, I led the overhaul and expansion of Social Security's suite of electronic services. I personally reviewed every major system before beta testing, and extensive beta testing often revealed the need for delays to make changes. We involved not only random focus groups, but also advocates for various people, such as victims of domestic violence.

We need to be very concerned about protecting the privacy of the data stored in these types of systems, which I believe are not adequately protected. The defense offered by the Center for Democracy & Technology and others—that the CMS systems are just a “routing tool,” not a repository—is either untrue or problematic. CMS needs to store data to create forensic trails necessary to track security breaches; failure to establish forensic trails would create a serious issue under the Federal Information Security Management Act of 2002.

We need to know whether unauthorized changes of insurance could leave Americans unexpectedly uninsured. We need to know how CMS will define and respond to breaches—I know how important that is because I suffered through OPM's inept response when my Federal financial records were breached 2 years ago. We need to know why many of the people who will deal with the public are just being hired now, and being hired without background checks. A rigorous authentication process may result in as many as 2 million people who will need to interact with CMS contractors when they fail to access the system—is CMS ready for that workload or are they going to sacrifice service or authentication? Greater transparency about these issues would improve the quality of the exchanges—and increase public confidence in the system.

Both SSA and the IRS formally appealed to OMB that the exchanges would violate the Privacy Act, violations which potentially carry criminal penalties. OMB eventually denied that appeal, but in my view HHS will be violating the Privacy Act on a massive scale by allowing people to make insurance decisions for other adult family members without their written consent. This feature of the system may well allow domestic abusers to track down their victims.

An August 2, 2013 inspector general report revealed that the CMS schedule has slipped so badly that mandatory security findings are scheduled for the day before implementation. With no room for adequate beta testing and revisions, HHS's claim that it will be ready to make security findings on its September 30 deadline is a fiction designed to preserve the larger fiction that the exchanges will be ready for uninsured Americans.

Before I conclude, I urge President Obama and Congress to scrutinize the performance of HHS Inspector General Levinson. Relying only on interviews and documents, his August 2, 2013 report on the exchanges contained less than 5 pages of analysis. His staff did not even try to use the beta version of the system.

HHS cannot have it both ways. If the exchanges can function on October 1, by July of this year there must have been a beta version. However, the inspector general did not inspect the beta version, and meekly noted that CMS withheld security documents. He ignored the vulnerabilities of a system that transmits, largely through the so-called “cloud,” sensitive personal information to CMS contractors and private insurers. He ignored the privacy issues, the security issues, and the issues associated with poorly screened and trained contractors. He did not assess usability, performance measures, governance, or contingency plans. With HHS's expanded role in health care, Americans need an inspector general who is a watchdog, not a lapdog.

Congress is bitterly divided about the Affordable Care Act, but there should be common ground. Whether or not you support an individual mandate, you can embrace the principle that no one should be forced to sacrifice privacy in order to comply with that mandate. To the best of my knowledge, work on systems that would comply with the Privacy Act stopped in early 2013 after OMB brushed aside the Privacy Act appeals of SSA and the IRS. A system respecting the Privacy Act would probably take an additional 6–18 months to develop.

President Obama has delayed other parts of the Affordable Care Act. Vulnerable Americans without lobbyists deserve the same respect and deference given to the business community. You should support a moratorium on the exchanges until HHS secrecy ends, and until we know whether uninsured Americans, will be forced to pay—along with their premiums—the high price of their privacy.

Thank you.

Mr. MEEHAN. Thank you, Mr. Astrue.

The Chairman now recognizes Dr. Parente for his testimony.

STATEMENT OF STEPHEN T. PARENTE, PH.D., MINNESOTA INSURANCE INDUSTRY CHAIR OF HEALTH FINANCE, DIRECTOR, MEDICAL INDUSTRY LEADERSHIP INSTITUTE, PROFESSOR, DEPARTMENT OF FINANCE, CARLSON SCHOOL OF MANAGEMENT, UNIVERSITY OF MINNESOTA

Mr. PARENTE. Thank you, Chairman Meehan, Ranking Member Clarke, and Members of the committee, for this opportunity to speak to you today.

My name is Steve Parente. I hold the Minnesota Insurance Industry Chair of Health Finance at the University of Minnesota. There, I serve as the professor in the Finance Department at the Carlson School and director of the Medical Industry Leadership Institute growing MBA program.

As I just stated, my expertise are health insurance, health information technology, and a medical technology evaluation. I have an appointment at Johns Hopkins University as a faculty member.

In the summer of 2011, I and my colleague from the Manhattan Institute, Paul Howard, wrote about implementation of the Affordable Care Act and security concerns regarding the Health Insurance Exchange Hub that is scheduled to be fully-operational in less than 20 days.

This essay received little attention at that time. On December 7, 2012, *USA Today* printed an op-ed written by Dr. Howard and myself that described the same issues as we did a year before. The 2012 op-ed received far greater attention Nationally and particularly from the administration.

The principal concern I sought to examine was the Government's capability to rapidly and securely combine information at a personal level from multiple Federal agencies in order to make eligibility determinations for Americans to purchase health insurance on a State or Federal insurance exchange.

I have stated and continue to posit that the combination of such data would be the largest personal data integration Government project in the history of this Republic with up to 300 million American citizens' records needing to be combined from several Federal agencies.

The Federal agencies involved in this integration are the Department of Health and Human Services to facilitate the data and operating parameters of the Federally-facilitated exchange and the State-based exchanges as well as insure that the applicants are not already eligible for Medicare benefits; the Social Security Administration to verify Social Security numbers, death indicator status, disability status under Title II of the Social Security Act, prisoner data or incarceration status, annual and monthly Social Security benefit information, and a confirmation to claim of citizenship is consistent with Social Security records; the Department of Treasury to verify income as well as transfer subsidies as necessary to purchase health insurance; the Office of Personnel Management, Peace Corps, and Department of Defense and Veterans Administration to make sure that applicants don't have access to health care coverage from other alternative sources; and finally, the Depart-

ment of Homeland Security to verify whether the individual is indeed legally present in the United States.

My expressed concern is that it is not clear how the data hub will operate. Ideally, the hub should function as a switch that routes information but does not retain the personal identifying information it is routing.

Major credit card purchases today operate this way where a retailer at the point of purchase uses your credit card to link a variety of data sources about you to make sure you are not a credit risk and then clears you to purchase for a large screen TV for the holidays.

This approach minimizes privacy risks and provides good data security, and the Federal data hub should operate this way, coupled to either a State or Federal insurance exchange as well as to the Social Security Administration, Treasury Department, Homeland Security, and Department of Justice, et cetera.

Operating this would create a fire-and-forget data system that would instantaneously link to an abstract piece of information and then delete it to prevent it from becoming a privacy concern.

Major financial services firms have been providing these services for nearly 2 decades, and if there ever has been a privacy breach, it is not from a pure data switch.

Now having said that about how one can provide reliable data protection, no one has said how this hub will actually operate to ensure that every precaution possible has been taken to avert privacy breaches as well as safeguard against identity fraud.

Greater transparency is needed as well as frank acknowledgment that the ACA's posted deadlines should take second place to reasonable data privacy and security concerns. This isn't a political point, it isn't meant to impinge on anyone's motives inside of HHS or the administration.

The fact that only a handful of individuals know truly how this will operate may preserve some security but it is operating as—not operating as planned, it could also be viewed as a failure with the execution for full transparency and provision of law that could—that had 3 years to implement but did not get the job done.

HHS's job is to implement this law and as much as some citizens may dislike an assortment of the law's underlying provisions, HHS' staff are doing exactly what they need to get it done under the constraints they can't control.

They are doing so in a politically-charged environment and crashing headlong into constraints of scarce human capital, complex regulatory environments, and of a massive IT project with literally no technical precedent.

I believe Congress has a legitimate oversight responsibility to ensure that whatever your feelings about the ACA, the final product is trusted, functional, and secure for all Americans. Congress should take that responsibility seriously and the administration should help them execute that responsibility.

In closing, I hope my efforts to bring transparency to operational parameters of the hub only strengthen its operation. Failure to build a secure hub could bring significant damage to the privacy and security of Federal data systems and cause irreparable harm

to Americans whose personal information would be lost to fraud and identity theft. This must not be allowed to occur.

Thank you for this opportunity to be heard today. I welcome your questions.

[The prepared statement of Mr. Parente follows:]

PREPARED STATEMENT OF STEPHEN T. PARENTE

SEPTEMBER 11, 2013

Thank you, Chairman Meehan, Ranking Member Clarke, and Members of the committee, for this opportunity to speak to you today.

My name is Steve Parente. I hold the Minnesota Insurance Industry Chair in Health Finance at the University of Minnesota. There, I serve as professor in the Finance Department at the Carlson School of Management and director of the Medical Industry Leadership Institute, a growing MBA program. My areas of expertise are health insurance, health information technology, and medical technology evaluation. I also have an appointment at the Johns Hopkins University in Baltimore, Maryland.

In summer 2011, I and my colleague from the Manhattan Institute Paul Howard wrote about implementation of the Affordable Care Act (ACA) and security concerns regarding the Health Insurance Exchange Hub that is scheduled to be fully operational in less than 20 days. This essay received little attention at the time. On December 7, 2012 *USA Today* printed an op-ed on written by Dr. Howard and myself that described the same issues as we did a year before. The 2012 op-ed received far greater attention Nationally and in particular from the administration.

The principal concern I sought to examine was the Government's capability to rapidly and securely combine information at a personal level from five Federal agencies in order for someone to purchase health insurance on a State or Federal exchange. I have stated and continue to posit that the combination of such data would constitute the largest personal data integration Government project in the history of the Republic, with up to 300 million American citizen records needing to be combined from five Federal agencies.

The five agencies involved in this integration are: The Department of Health and Human Services, to facilitate the data and operating parameters of the exchanges; the Social Security Administration, to verify if the person to be insured is indeed living; the Department of Treasury, to verify income level, as well as transfer subsidies as necessary to purchase health insurance; the Department of Justice, to verify that the insured is not incarcerated; and finally, the Department of Homeland Security, to verify the citizenship of the individual.

My expressed concern is that it's not clear exactly how the data hub will operate. Ideally, the hub should function as a switch that routes information but does not retain the person-identifying information it is routing. Major credit card purchases today operate this way: Where a retail vendor, at the point of purchase, uses your credit card to link a variety of data about you to make sure you are not a credit risk and then clears you for purchase of your 70" LCD TV for the holidays. This approach minimizes privacy risks and provides good data security.

The Federal data hub should operate this way, coupled to either a State or Federal insurance exchange as well as to the Social Security Administration, Treasury Department, Homeland Security, and Department of Justice, et al. Operating this would create a fire-and-forget data system that would instantaneously link to an abstract piece of information and then delete it to prevent it from becoming a privacy concern. Major financial services firms have been providing these services for nearly 2 decades, and if there ever has been a privacy breach, it is not from a pure data switch.

Having said how you could provide reliable data privacy protection, no one has said how the data hub will actually operate to ensure no privacy breaches as well as safeguard against identity fraud. Greater transparency is needed, as well as a frank acknowledgement that the ACA's posted deadlines should take second place to reasonable data concerns. This isn't a political point, and isn't meant to impinge upon anyone's motives inside HHS. The fact that only a handful of individuals know truly how this will operate may preserve some security. Alternatively, if the hub does not operate as planned, it may also be viewed as a failure to plan and execute with full transparency a provision of the law the agencies had over 3 years to implement.

HHS' job is to implement the law. As much as some citizens dislike an assortment of the law's underlying provisions HHS staff are doing exactly what they are sup-

posed to do and facing constraints they can't always control. They are doing so in a politically-charged environment—and crashing headlong into the constraints of scarce human capital, complex regulatory requirements, and a massive IT project with literally no technical precedent.

I believe Congress has a legitimate oversight responsibility to ensure that—whatever your feelings about the ACA—the final product is trusted, functional, and secure for all Americans. Congress should take that responsibility seriously—and the administration should help them execute that responsibility.

In closing, I hope my efforts to bring transparency to operational parameters of the hub only strengthen its operation. Failure to build a secure hub could bring significant damage to the security of Federal data systems. This must not be allowed to occur.

Thank for you this opportunity to be heard today. I welcome any questions.

Mr. MEEHAN. Thank you, Dr. Parente.

The Chairman now recognizes that the gentlelady from the IG's office, Ms. Daly.

**STATEMENT OF KAY DALY, ASSISTANT INSPECTOR GENERAL,
AUDIT SERVICES, U.S. DEPARTMENT OF HEALTH AND
HUMAN SERVICES**

Ms. DALY. Thank you, Chairman Meehan.

Thank you, Chairman Meehan, Ranking Member Clarke, and other distinguished Members of the subcommittee. I appreciate the opportunity to be here today to discuss the Office of Inspector General's review of the Centers for Medicare and Medicaid Services implementation of the Data Services Hub from a security perspective.

My testimony today summarizes OIG's observations about CMS' progress in implementing security requirements of the hub including a recent update we received from CMS management on the status of the project.

As you know, the hub plays a key role in providing important data for health insurance exchanges that are also called marketplaces, which are being established under the Affordable Care Act.

The State-based exchanges will serve as the one-stop shop where individuals will get information about their health insurance options, be assessed for eligibility, and enroll in the health plan of their choice.

The hub is intended to support those exchanges by providing a single point where exchanges can access data from different sources including Federal agencies and their State partners.

It is important to note that the hub does not store data, rather, it simply acts as a conduit for the exchanges to access data from where they are stored.

In a report issued on August 2, 2013, we assessed the information technology security controls that CMS was implementing for the hub and the coordination between CMS and Federal and State agencies during the development of the hub. We did not review the functionality of the hub or privacy issues associated with it.

At the time of our reviews, CMS was addressing and testing security controls of the hub during the development process. Several critical tasks remained to be completed at the time, such as the final independent testing of the hub security controls, remediating the security vulnerabilities identified during testing, and obtaining the security authorization for the hub before opening the exchanges.

CMS' schedule at that time was to complete all of these tasks by October 1 in time for the expected initial open enrollment date for the health insurance exchanges.

Our report described the time lines that CMS provided us for its system security plan, its risk assessment, and its security control assessment and security authorization decisions.

In our report, we noted that between March and July, some key dates had moved back. These were internal target dates set by CMS for these milestones and not mandated deadlines.

Subsequent to issuing our report, CMS has reported to us that it has made additional progress on these key security milestones. For example, since our review, CMS has reported to us that the security authorization was completed on September 6, 2013. We have not independently verified CMS' progress since completing our audit.

Our review also observed that CMS was coordinating with its Federal and State partners during the development and testing of the hub in part to ensure that security measures were implemented by all stakeholders.

CMS had developed a testing approach and test plans for the inter-agency testing aspect. At the time of our reviews, CMS was in the process of executing those test plans.

In addition, CMS has developed security-related documents and security agreements regarding its Federal partners and information systems and networks.

Federal policy does require agencies to develop interconnection security agreements for Federal information systems and networks that share or exchange information.

Each of the Federal partners will provide information on their systems' environments and the overall approach for safeguarding the confidentiality, integrity, and availability of shared data in systems interfaces.

Since our review, CMS has reported to us that all of these agreements are expected to be approved by September 27, 2013.

In closing, I want to thank you for your interest in our work on this important subject and the opportunity to be part of this discussion. I would be very pleased to take any questions you might have.

[The prepared statement of Ms. Daly follows:]

PREPARED STATEMENT OF KAY DALY

SEPTEMBER 11, 2013

INTRODUCTION

Good afternoon, Chairman Meehan, Ranking Member Clarke, and other distinguished Members of the subcommittee. Thank you for the opportunity to testify about the Office of Inspector General's (OIG) review of the Centers for Medicare & Medicaid Services' (CMS) implementation of the Data Services Hub (hub) from a security perspective, which we issued on August 2, 2013.¹ My testimony today summarizes OIG's observations about CMS's progress in implementing security require-

¹*Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange—Data Services Hub*, A-18-13-30070, August 2013, available on-line at <https://oig.hhs.gov/oas/reports/region1/181330070.asp>.

ments of the hub during the period of our review.² We assessed the information technology (IT) security controls that CMS was implementing for the hub, adequacy of the testing being performed during its development, and the coordination between CMS and Federal and State agencies during the development of the hub. We did not review the functionality of the hub or issues specific to the Privacy Act.

At the time of our review, CMS was addressing and testing security controls for the hub during the development process. Several critical tasks remained to be completed, such as the final independent testing of the security controls, remediating security vulnerabilities identified during testing, and obtaining the security authorization decision for the hub before opening the exchanges. CMS's schedule at that time was to complete all of these tasks by October 1, 2013, in time for the expected initial open enrollment date for health insurance exchanges.

Our report described the time lines that CMS provided us for its system security plan, risk assessment, security control assessment, and security authorization decisions. In our report, we noted that between March and July, some key targets had been shifted to later dates. These were internal target dates set by CMS for these milestones and not mandated deadlines. Since issuing our report, CMS has reported to us that it has made additional progress on these key milestones, including obtaining its security authorization for the hub on September 6, 2013. We have not independently verified CMS's progress since completing our audit.

Following is a discussion of the hub's role within the health insurance exchanges, the results of our review, and concluding observations.

BACKGROUND

States must establish health insurance exchanges by January 1, 2014,³ and all health insurance exchanges must provide an initial open enrollment period beginning October 1, 2013 (45 CFR § 155.410). Health insurance exchanges, also known as Marketplaces, are State-based competitive marketplaces where individuals and small businesses will be able to purchase private health insurance.⁴ Exchanges will serve as a one-stop shop where individuals will get information about their health insurance options, be assessed for eligibility (for, among other things, qualified health plans, premium tax credits, and cost-sharing reductions), and enroll in the health plan of their choice.

The hub is intended to support the exchanges by providing a single point where exchanges may access data from different sources, primarily Federal agencies. It is important to note that the hub does not store data. Rather, it acts as a conduit for exchanges to access the data from where they are originally stored. Hub functions will include facilitating the access to data by exchanges, enabling verification of coverage eligibility, providing a central point for the Internal Revenue Service (IRS) when it asks for coverage information, providing data for oversight of the exchanges, providing data for paying insurers, and providing data for use in web portals for consumers.

Effective security controls are necessary to protect the confidentiality, integrity, and availability of a system and its information. The National Institute of Standards and Technology (NIST) developed information security standards and guidelines, including minimum requirements for Federal information systems. CMS is required to follow the NIST security standards and guidelines in securing the hub.⁵

To determine CMS's progress in implementing security requirements for the hub, OIG reviewed documentation, project schedules, and time lines; interviewed CMS employees and contractors and personnel from key Federal agencies working with CMS during development of the hub; and reviewed CMS's security testing results.

²We performed our fieldwork substantially from March through May 2013. We continued to receive updates from CMS through July 1, 2013, and its comments on our draft report are included in the final report.

³The Patient Protection and Affordable Care Act § 1311(b) (Pub. L. No. 111-148) and the Health Care Reconciliation Act of 2010 (Pub. L. No. 111-152), collectively known as the Affordable Care Act (ACA).

⁴A State may elect to operate its own State-based exchange or partner with the Federal Government to operate a State partnership exchange. If a State elects not to operate an exchange, the Department of Health and Human Services will operate a Federally Facilitated Exchange. For the purposes of this report, "exchanges" refers to all three types of health insurance exchanges.

⁵NIST's security standards assist Federal agencies in implementing the requirements under the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, et seq.

RESULTS OF OIG'S REVIEW

At the time of our review, CMS and its contractors were continuing to develop the hub and work with its Federal and State partners in testing the hub to ensure its readiness in time for the initial open enrollment to begin on October 1, 2013. The following observations provided the status of CMS's implementation related to security controls, security testing, and coordination at the time of our fieldwork.

Security Authorization

According to NIST security standards, every Federal information system must obtain a security authorization before the system goes into production. The security authorization is obtained from a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations. At CMS, the authorizing official is the Chief Information Officer (CIO).

The security authorization package must include a system security plan, information security risk assessment, and security control assessment report. The security authorization package provides important information about risks of the information system, security controls necessary to mitigate those risks, and results of security control testing to ensure that the risks have been properly mitigated. Therefore, these documents must be completed before the security authorization decision can be made by the authorizing official. Under the NIST guidelines, the authorizing official may grant the security authorization with the knowledge that there are still risks that have not been fully addressed at the time of the authorization.

At the time of our review, the security authorization decision by the CMS CIO was expected by September 30, 2013. Since our review, CMS has reported that the security authorization was obtained on September 6, 2013.

System Security Plan and Information Security Risk Assessment

CMS incorporated the elements required for adequate security into the draft hub system security plan. The plan: (1) Provides an overview of the security requirements of the system, (2) describes the controls in place or planned (e.g., access controls, identification, and authentication) for meeting those requirements, and (3) delineates the responsibilities and behavior expected of all individuals who access the system.

CMS was still drafting the information security risk assessment at the time of our review. For this reason, we could not assess CMS's efforts to identify security controls and system risks and implement safeguards and controls to mitigate identified risks. Key aspects of the assessment should identify risks to the operations (including mission, functions, image, or reputation), agency assets, and individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

At the time of our review, the CMS contractor did not expect to be able to provide finalized security documents, including the system security plan and risk assessment, to CMS for its review until July 15, 2013. Since our review, CMS reported to us that the documents were provided to CMS on July 16, 2013.

Security Control Assessment and Testing

At the time of our review, CMS and its contractors were performing security testing throughout the hub's development, including vulnerability assessments of hub services. CMS was logging and tracking defects and vulnerabilities, as well as correcting and retesting hub services to ensure that vulnerabilities are remediated.

A security control assessment of the hub must be performed by an independent testing organization before the security authorization is granted.⁶ The assessment determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome of meeting the security requirements for the information system. The goal of the security control assessment test plan is to explain clearly the information the testing organization expects to obtain prior to the assessment, the areas that will be examined, and the activities expected to be performed during the assessment.

According to CMS, the assessment was scheduled to be performed between August 5 and 16, 2013. Since the assessment was not completed at the time of our review, we could not determine whether vulnerabilities identified by the testing would be mitigated. Since our review, CMS has reported to us that the assessment was completed on August 23, 2013.

⁶NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Revision 1.

Adjustments to CMS Time Lines

CMS provided us with time lines in March 2013 and May 2013 for its system security plan, risk assessment, security control assessment, and security authorization decisions. CMS also provided us additional information on timing of certain steps after the May time line. Some key targets had been moved to later dates as the development of the hub was continuing. It is important to note that these were internal target dates set by CMS for these milestones and not mandated deadlines.

For example, in March, the security control assessment test plan was targeted to be provided to CMS on May 13, 2013, and this due date was subsequently moved to July 15, 2013, and the start date of the security control assessment was moved from June 3, 2013, to August 5, 2013. CMS stated that the security control assessment time frame was moved so that performance stress testing of the hub could be finished before the assessment and any vulnerabilities identified during the stress testing could be remediated. Otherwise, CMS might need to perform an additional assessment after the remediation was complete.

According to CMS's time line from May 2013, the security authorization decision by the CMS CIO was expected on September 30, 2013. OIG noted in our report that if there were additional delays in completing the security authorization package, the CMS CIO may not have a full assessment of system risks and security controls needed for the security authorization decision by the initial open enrollment period set to begin on October 1, 2013. In its comments on our draft report, CMS stated that it was confident that the hub would be operationally secure and it would have a security authorization before October 1, 2013.

Since our review, CMS has reported to us that the security authorization was obtained on September 6, 2013.

Coordination Between CMS and Its Federal and State Partners

Our review observed that CMS was coordinating with its Federal and State partners during the development and testing of the hub, in part to ensure that security measures are implemented by all stakeholders. CMS developed an approach for interagency testing and has developed test plans. At the time of our review, CMS was in the process of executing its test plans, which included testing for secure communications between CMS and its Federal and State partners and performance stress testing of the hub. In addition, CMS has developed security-related documents and security agreements regarding Federal information systems and networks. The Federal partners are the IRS, Social Security Administration (SSA), Department of Homeland Security (DHS), Veterans Health Administration (VHA), Department of Defense (DoD), Office of Personnel Management (OPM), and Peace Corps.

CMS has developed security-related documents related to the hub and the exchanges. CMS developed Interface Control Documents (ICD) with all of its Federal partners. The ICDs provide a common, standard technical specification for transferring ACA-related information between CMS (the hub) and its Federal partners. The ICDs establish standard rules, requirements, and policies (including security-related policies) with which the development and implementation of the interfaces between CMS and its Federal partner must comply. CMS and its Federal partners collaborated in developing the ICDs and signed the ICDs in May 2013.

Federal policy requires agencies to develop Interconnection Security Agreements (ISAs) for Federal information systems and networks that share or exchange information with external information systems and networks.⁷ The Master ISA describes the systems' environment; the network architecture; and the overall approach for safeguarding the confidentiality, integrity, and availability of shared data and system interfaces. In addition, the Master ISA contains information on CMS information security policy and the roles and responsibilities for maintaining the security of ACA systems.

CMS completed a preliminary review of the Master ISA between CMS and the developer of the hub on April 2, 2013, and the Associate ISAs on May 15, 2013. Each of the Federal partners will provide similar information pertaining to the partner agency in the Associate ISAs, which will be signed by the Federal partner authorized official. Since our review, CMS has reported to us that all ISAs with its Federal partners are expected to be approved by September 27, 2013.

A service-level agreement (SLA) is a negotiated agreement between a service provider and the customer that defines services, priorities, responsibilities, guarantees,

⁷Specifically, Office of Management and Budget Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their IT systems to other systems. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection.

and warranties by specifying levels of availability, serviceability, performance, operation, or other service attributes. A SLA is needed between CMS and each of its Federal partners to establish agreed-upon services and availability, including response time and days and hours of availability of the hub and the Federal partner's ACA systems. According to CMS's project schedule, the SLA with IRS was completed on March 15, 2013; the SLA with DHS was expected to be signed by July 26, 2013; and the SLA with SSA was expected to be signed by September 27, 2013. The SLAs with the remaining Federal partners (VHA, DoD, OPM, and Peace Corps) were expected to be signed by September 20, 2013. Since our review, CMS has reported to us that the SLAs with IRS, VHA, and DHS are expected to be signed before the end of September. CMS also reported that DoD-Tricare and CMS have agreed to allow transactions to occur and monitor the "response time metric" to set a baseline for the interaction standards before they execute their SLA. They expect to execute their SLA by the end of December.

CONCLUDING OBSERVATIONS

CMS is taking steps to ensure that there are adequate security measures for the hub in compliance with NIST guidelines. At the time of our review, CMS was working with very tight deadlines to ensure that security measures for the hub were assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013.

Our report provided the status of the implementation of key security requirements at a point in time. CMS has reported to us that it has completed all of the required steps and obtained its security authorization on September 6, 2013. We have not independently verified CMS's progress since completing our audit.

Thank you for your interest in our work on this important issue and the opportunity to be a part of this discussion. I would be pleased to answer your questions.

Mr. MEEHAN. Thank you, Ms. Daly.

The Chairman now recognizes our last panelist, Mr. Salo.

Mr. Salo—

STATEMENT OF MATT SALO, EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION OF MEDICAID DIRECTORS

Mr. SALO. Great. Thank you very much, Chairman Meehan, Ranking Member Clarke, other Members of the committee and subcommittee.

My name is Matt Salo. I am the Executive Director of the National Association of Medicaid Directors. I appreciate the opportunity to testify on their behalf.

It is important to talk a little bit about what Medicaid is; why is Medicaid here at this conversation about the hub? Medicaid itself does a lot more than most people think.

We deal in numbers of that are astronomical. We are going to spend close to \$500 billion this year covering 72 million Americans. It is a State and Federal program. Our members are the ones in every State and territory who actually administer the program.

We are here in large part because again, not very well-known, but Medicaid really is kind of the centerpiece of the ACA. The ACA spent about \$1 trillion over 10 years, half of that goes into Medicaid, to the expansion, and for other changes to it.

So obviously, the ACA or Obamacare is a highly politically-charged issue. We know this, but what is also true is that the impacts of the law are very real and are very real for the citizens of this country, the citizens of each one of our States.

For my members, as public servants, their primary job is to uphold the law but also to ensure the health and the well-being and yes, the security of their citizens.

If things don't go well, we get the calls. So it is very, very important that we make sure that things do go as well as possible, and there is going to be a lot of aspects of that.

I think the primary ones for this issue are that our citizens not only understand but are able to access, afford, and be safe in their security in terms of the new health options that are going to be available to them.

So while there has been a lot of talk and a lot of attention to bigger picture issues like the expansion and State versus Federal exchanges, we welcome the opportunity to talk about some of these under-the-hood types of conversations and the work that is going on.

Other panelists have talked about the Herculean nature of what we are building here, the unprecedented nature. We have bandied around terms like moonshot earlier.

There really is no precedence in terms of what we are trying to build here, and I think it is important to keep all of that in mind especially when confronting the fact that I think at least at the onset, people were envisioning that this was going to be a Travelocity of health care.

While I think we may get there someday, I do not think it will look like that on Day 1 because in many ways, what is happening is the creation of the system is kind of like building a bridge starting at opposite ends of a river and trusting that they meet in the center.

The challenge for Medicaid is that in many ways it is building 56 different bridges and hoping and trusting that they will meet in the center. The challenges obviously are that there is never enough time, never enough money, never enough bandwidth to do all of these things.

But having said all of that, again, this has been issue No. 1 for our members for the past several years. While there are many aspects of this, security is a very, very important one as well.

It is important to know that from our perspective as we build the connectivity between Medicaid and the hub, the concepts of the security of the information are being baked in to that connectivity, and that the security and the privacy and the confidentiality of information is not something that is new to us.

We served 72 million people last year and we did so in a way that bridged lots of different gaps. Medicaid was able to communicate with other programs like TANF for food stamps, SNAP.

Medicaid was able to bridge the gap with Medicare to ensure care coordination for dual eligibles. Medicaid is able to bridge the gap with private insurance to do third-party liability, to look at citizenship documentation and that became part of the law a couple years ago, and in many of the aspects of program integrity that State and Medicaid programs take very, very seriously.

This is a very, very important issue and it will be addressed and it will be one of the core functions of what we do.

By all that, I do want to say though that when we are looking at October 1 or January 1, it is important to recognize that we are going to have a turbulent takeoff and we are going to have a bumpy road as we move forward because of the complexity of what we are doing, because of the nature of what we are doing.

But I think it is also important to note that from our perspective, we do not believe that security is one of those things that is going to be sacrificed or jettisoned in order to get this done right on time.

That in fact we think there will be a lot of Day 2, Day 3, Day 4 mitigation plans and work that is being done, work that is being planned as we speak to try to figure out how do we take what we know will break down and fix it.

Again, not on the security side, but in terms of the consumer interface where we know that people's lives, people's situations are messier than rules engines can usually handle, but we are working on this. This is what we do.

I would just close with an analogy, you know, in some sense, what we are doing here is analogous to rolling out the Medicare Part D program.

Although that seemed relatively straightforward, on Day 1 when we turned on all the lights, it was a bit of a mess, and we had a lot of seniors who were in pharmacies who didn't know what was going on, couldn't get their prescriptions, couldn't get anyone to give them clear answers.

It was the States, the Feds, and the plans who worked together tirelessly for months to figure out, how do we fix this? Now, in many respects, this is like Part D on steroids, but that is the commitment we have, and that is the vision that we see moving forward.

This will work. It will not work perfectly. We do not believe security is going to be a primary concern on Day 1, and we will fix what happens and what breaks as we move forward.

Thank you, and I am happy to answer any questions.

[The prepared statement of Mr. Salo follows:]

PREPARED STATEMENT OF MATT SALO

SEPTEMBER 11, 2013

Good afternoon Chairman Meehan, Ranking Member Clarke, and distinguished Members of the subcommittee. My name is Matt Salo, and I am the executive director of the National Association of Medicaid Directors (NAMD). I appreciate the opportunity to testify before you today.

MEDICAID

Medicaid is the Nation's health care safety net. Jointly financed by the States and the Federal Government, Medicaid spent more than \$420 billion last year to provide health care to more than 72 million Americans. The program is administered by the States within a broad Federal framework which leads to enormous variation across States in terms of who is covered, what services are provided, and how those services are paid for and delivered. Furthermore, within any given State, Medicaid's role is broad, varied, and complex. Medicaid funds close to 50 percent of all births, and the majority of all publicly-financed long-term care in this country.

It also provides most of the Nation's funding for HIV/AIDS-related treatments, mental health services, and others.

It is therefore very difficult to talk simplistically about Medicaid (either Nationally, or within a State), despite its incredible importance in the U.S. health care system.

NAMD was created with the sole purpose of providing a home for the Nation's Medicaid directors and we represent all 56 of the State, territorial, and DC agency heads. Our two broad objectives are to give the Medicaid directors a strong, unified voice on National and Federal matters as well as helping develop a robust body of technical assistance and best practices for them to improve their own programs. While no two programs look exactly alike, the directors are unified in their heartfelt

desire to improve the health and health care of the growing number of Americans who rely on the program.

IMPLEMENTING THE AFFORDABLE CARE ACT—OVERVIEW

No issue has been more polarizing in recent memory than the Affordable Care Act (ACA), often known as “Obamacare.” While the ACA may not be wildly politically popular, or even well-understood, it is the law of the land, and it will have far-reaching and fundamental impacts on the citizens of every State in the Nation.

Politics aside, the key to the success or failure of this new law lies in how well it serves our citizens; and how well they are able to understand, access, and afford their new health insurance options. In many ways much of the foundation hinges on reforms to the Medicaid program. The States have been working as quickly and effectively as possible for months, even years, to put together the pieces of this complex health insurance overhaul.

To fully understand the Herculean task the ACA presented to State Medicaid programs, we must acknowledge that States began this journey from very different starting points. Likewise, even several years after the official ACA launch we can still expect to see differences in the structure of Medicaid programs—and health care systems generally—as States determine how to best meet the diverse needs of their citizens.

Regardless of their starting or ending points, there is a long list of changes that all States have to make to comply with the law. These include overhauling complex eligibility systems to conform to new standardized Federal rules. State Medicaid agencies also have been working to integrate with new health insurance marketplaces to ensure that individuals and families receive consistent, accurate information about their eligibility for public insurance programs. And they have endeavored to minimize the burden and confusion for individuals and families trying to navigate the rules for these new programs.

Investments in this system overhaul are being made by States, and by the Federal Government—with everyone involved fully committed to ensuring that they work as well as possible. As envisioned, the new system would be able to process a few consumer data points (name, Social Security number) and determine the insurance program—Medicaid or the marketplace—for which each individual in a family would be eligible. It also would begin the actual process of enrolling and paying for that coverage.

Achieving this vision requires real-time communication between States and the Federal Government and among multiple Federal departments that historically have never talked to one another. In many States, it requires a complete overhaul of decades-old Medicaid eligibility systems in order to interface with a new Federal “hub.”

In addition to these technical hurdles, there is another reality to contend with: No two State Medicaid programs are alike. These differences have developed over the nearly 50 years of the program’s existence, and reflect the political and cultural dynamics of each State. These differences range from who is covered, which benefits are available and how care is both delivered and paid for, as well as the sophistication (or too often, lack thereof) of the State eligibility and information systems, many of which were built in the 1980s.

In a sense, States are building 50+ bridges all at the same time, from different starting points and hoping that these efforts meet exactly in the middle. These bridges CAN be built and they are in fact being built now. But it is vitally important that we take heed of the lessons of complex policy implementations in the past as well as the expertise States have with program and system implementations.

PRIVACY, SECURITY, CONFIDENTIALITY OF INFORMATION

Security, privacy, and confidentiality are among the highest priorities for State Medicaid Directors. They also hold their vendors to the same high expectations and work with them to ensure they too appropriately safeguard personal information.

While there have been security breaches in Medicaid, there have also been security breaches in the banking and credit card industries, with internet service providers, and practically every other component of our increasingly interdependent economy. It is unrealistic to expect that these things can be prevented entirely, it is more important that we focus on how to minimize and mitigate the risks that are inherent in an interconnected society.

States currently handle many of these types of information in a highly secure way as they make eligibility determinations for the more than 70 million Americans currently on the program. States routinely work with chief information officers, con-

sumer protection agencies, the inspector general's offices in a variety of State and Federal agencies, and more in their efforts to protect consumer information.

While the specifications of the systems being built to interface with the Federal data hub and the Insurance Marketplaces are new, States have decades of experience working across program platforms to ensure privacy, confidentiality, and security of patient information (medical and otherwise). Whether its communicating with private insurance companies to do third-party liability determinations, working with other programs such as TANF or SNAP to eliminate redundancies, working with a range of Federal agencies to implement citizenship documentation requirements, or working with Medicare to improve care coordination for individuals dually eligible for both programs, State Medicaid directors have significant experience and perspective.

In each of these examples, it is important to note that the sharing of information across programs or payors is a vitally important function. In fact, the entire field of public health and program integrity would barely exist if data could not flow securely, quickly, and effectively.

While I am not here to testify to the readiness schedule of the Federal data hub, we do know from experience of the high-level commitment to privacy and security. In fact, this commitment is one of the main drivers of our concern that the full range of operational capacity is not likely to be met by October 1. In fact, some of the earliest conversations with our Federal partners revealed a significant stance on behalf of IRS that it was more important to ensure that the exchange of data was done securely than it was to do it quickly.

THE ROAD AHEAD

As we approach the open enrollment date of October 1, 2013, there is one lesson that clearly stands out: We must be prepared for a turbulent take-off.

The magnitude of the changes and the many different pieces that have to be linked together mean everyone—consumers, policymakers, and other interested stakeholders—must have reasonable expectations of the systems and programs early on. In many instances, the consumer experience will not be immediately smooth. Real people are going to be frustrated when accessing the system. Whether it's a failure of computer algorithms to properly account for the startling complexity of real people's lives, or the difficulty in ensuring that these multiple State and Federal agencies are communicating in real time, it will be bumpy.

However, it's also reasonable to expect that the experience can and will improve over time. As they do in advance of any major implementation, Medicaid agencies are trying to predict, plan for and set up procedures to resolve the problems that will inevitably arise. At the same time they will continue working towards the ultimate goal of compliance with the law's requirements and seizing other opportunities they've identified.

The health and safety of Medicaid clients is the main concern of Medicaid directors, and they will continue their on-going commitment to provide the best possible service to beneficiaries, while protecting the integrity of the program, and being responsible stewards of taxpayer dollars.

Mr. MEEHAN. Well, thank you Mr. Salo.

I thank all of the panelists for their testimony.

Let me begin, Mr. Salo, you made an observation and I think it was really important to recognize that some of the people that are at the most risk here are those in Medicaid, the poorest, those in the least capacity to be able to recover or help themselves in situations where they may be taken advantage of.

You used the word "no precedence in its size." Dr. Parente called it I think the greatest—the "largest personal data Government integration project in the history of the Republic."

Ms. Daly, let's get the elephant out of the room. You know, we are talking here about representations that have been made by an agency and findings that you made about their readiness to meet these deadlines.

But we had the IG before us just a few weeks ago, the HHS itself said, and your reports confirmed they would not be ready until the 30th at the end of this month.

That is in the course of the normal business. We know the challenges. I am already suggesting this is the largest database in the history of the Republic.

Now, we received a report which you just said that lo and behold it was done on the 6th. They are ready to go.

Now this is an agency who for 3 years failed to meet a single deadline, and in your own IG's report and virtue of every single deadline that was articulated as much as 3 months before there was not a single deadline met.

Now you have stated yourself that this has not been done with any independent verification and the word continues to be just "trust us."

Ms. DALY, you are the Inspector General. Do you trust them?

Ms. DALY. Chairman Meehan, I appreciate the opportunity to respond to that. In our report, we did point out that they had—some of the dates had moved from their original plan date.

In fact, the date for the security authorization that was recently provided on September 6, in our report, we pointed out that it was—that is on September 30—so that is what gave us pause and wanted to get that—the early information out to the Members of this oversight body so that steps could be at taken and pressure to bear where appropriate.

So with that, we have recently been provided the assurance from the CIO at CMS through that security authorization decision, that is part of the normal NIST standards that are used and NIST, as you know, sir, it is the National Institute—

Mr. MEEHAN. I know those—

Ms. DALY. Yes, sir, very good. So with that, you know, we are just providing that information to you. We have not had a chance to go in and do a thorough assessment of it at this time given the short time span.

Mr. MEEHAN. So you have passed this on, but let's go through. Now what are the three steps? We understand that there are three steps in a NIST process.

There is the identification of the program that we have. There is beta testing of that program. Once that is beta tested, you identify the flaws in that program, you then fix that program, you then test it again to assure—and it is at that point in time that there is the certification.

They were not even ready at that point in time, which was only 2 or 3 weeks ago to certify to us that they had even done the appropriate beta testing.

Now you tell me how it is; we need your help. You are the person who is the independent verification, not just "trust us." So how can we believe that what was originally scheduled not to be done 'til the 30th on a massive project in which they have failed to meet a single deadline has been done on the 6th and they have failed to give you any information as we said, did you get, when you asked for information about the documents—Mr. Astrue identified them specifically—you were not given those documents. They were held back from you. You are an Inspector General. Why wasn't a demand made for those documents?

Ms. DALY. Well, sir, actually, to be clear, in our report, we discuss a number of documents that weren't available at the time—

Mr. MEEHAN. Well, if they are not available then, what makes you think that they were? Because that is part of the legal obligations. This isn't something that they just get to decide. They are going to determine how this process takes place. That is the NIST standards.

Do you believe that they made up all of that ground in that short period of time?

Ms. DALY. Well, sir, I can't speak to that at this time.

Mr. MEEHAN. What does your gut tell you?

Ms. DALY. I don't have a reaction. I generally, you know, being an auditor, I base our work on, you know, the generally accepted auditing standards and that is how we go about and do our work and I would have to go in and do a number of procedures in order to report back to—

Mr. MEEHAN. One of them might be real beta testing. Do you intend in light of what they—they have just made representations to you, we still have a period, do you intend to have the inspector general's office use all of its resources to do the actual beta testing of certain parts of the facility before October 1?

Ms. DALY. Well, sir, let me clarify for you that the beta testing is generally focused on the functionality of the system and with the functionality of the system, that is really more about how the user experiences that system and so forth.

Mr. MEEHAN. But not security—

Ms. DALY. It is not really security.

Mr. MEEHAN. So we haven't even tested for security.

Ms. DALY. Well, sir, to be—one of the key elements that the CIO should be considering as part of his security authorization decision is the independent security testing of its being done, and I want to highlight that it is independent, being done by a contractor, so that that provides that independent assurance to the CIO in performing that. But again, we have not seen the results of that.

Mr. MEEHAN. Okay. My time has expired.

I now recognize the Ranking Member, the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

Ms. DALY, I just want to get some fundamental facts from you. If you can just give us a definition of the OIG's role in the marketplace and exchange and the Federal data hub, what exactly is OIG's role there?

Ms. DALY. Well, with regard to that, the OIG, as you know under the Inspector General Act, has certain responsibilities for fighting waste, fraud, and abuse, and protecting the health and safety of the you know, people and beneficiaries—the U.S. taxpayers basically—and all of our citizens.

That is where we emphasize. We don't have a role in the operation whatsoever. So it is very important that we maintain our independence in order to provide such an independent assessment when it is appropriate to do so.

Ms. CLARKE. So would you state that your role has not been fully activated yet just in light of the fact that No. 1, the data hub is just coming on-line, and the marketplaces are beginning to emerge now?

Or are you giving oversight to this process and looking or scrutinizing the process to see whether in fact it is efficient or effective? Where do you see yourselves right now? What is the office doing at this particular point in time?

Ms. DALY. Well, at this particular point in time, we have been, as you know, monitoring the situation because it is unfolding daily, you know, trying to stay abreast of some of the prior work that had been done, looking forward and doing risk assessments on what is the appropriate use of our resources because our resources are stretched pretty thin.

We have also been and I want to highlight this for the Members today, you know, coordinating with GAO, with State auditors, and with other inspector generals because we see that as critical because this, is as everyone has noted, a huge enterprise.

Ms. CLARKE. So can you tell us about how you have performed your audit of the hub preparations and testing?

Ms. DALY. Certainly. Our work really followed the generally accepted Government auditing standards, and to do so, what we did is we were coordinating with GAO. GAO was in there reviewing the data hub and certain aspects of the exchanges through a, you know, a request that they had received.

So we coordinated with them—I am sorry—to ensure that we didn't duplicate any effort. You know, we have got a lot of the ground to cover, so we want to make sure that our work is complementary, not duplicative.

So in that regard, they were doing certain aspects. They advised that they were not looking at the security over the hub, so we said, all right, we will look at the security over the hub.

So we designed a program to ensure that the agents—to be able to assess whether the agency was in fact following the NIST standards in that regard.

Ms. CLARKE. So why did you, as some suggest, just briefly note in the audit that you did not have access to the CMS security documents?

Ms. DALY. Well, Ranking Member Clarke, in our report we indicated that the agency had not provided us certain documents at that time. I think one of them specifically was a security test plan because it wasn't available at that point in time.

Then, you know, of course subsequently, it may have become available. It wasn't that they refused, it just wasn't available.

Ms. CLARKE. Okay. Is it available now?

Ms. DALY. It could be. I think if we requested—I am pretty comfortable it has been available now. They have provided us some updates of data that you know, has subsequently been done and some of the dates it was done on.

Ms. CLARKE. Can you, again, just give us a sense of why you didn't engage the beta testing on the hub?

Ms. DALY. Well, we didn't engage that part because No. 1, that is usually towards the end of the project and our work primarily wrapped up really by the end of June.

We got, you know, a quick update of certain dates before we published the report, but most of the work was done a bit earlier and some of that information and certainly any sort of beta version wasn't available.

The other part would be that that would cover more functionality issues too, and that was really beyond our scope because we were, as we understood it, GAO would have been looking more at the functionality over the hub. We were focused on the security over the hub.

Ms. CLARKE. So is it that to a certain degree, there are some theoretical aspects to I guess standing up the hub that makes it somewhat exercise of futility for us to begin the testing?

Or is it that you are waiting for a certain level of the operation to be complete before the testing becomes applicable? I am not clear on that.

Ms. DALY. I appreciate that. The issue is there are certain aspects of testing that cannot be done until the process is far enough along; until enough has been built in order to do any testing.

Now to be clear, part of our audit approach was to look at the testing that was on-going by the agency as it was being built because the agency employed a—actually, it is a system development process called Agile, and it is very popular right now because you can build things out fairly quickly.

With that though, they are doing continuous testing as it goes on, but this is by, if you will, development personnel. So what happens later on then is all independently confirmed, in accordance with what NIST calls for, and an independent security assessment that is done after all of the internal testing is done.

So with that, you know, we said there wasn't any time for us to go in and do it, and we didn't want to duplicate any effort that was on-going. Instead, we reviewed the documents that they had available.

For example, as part of their on-going testing, we looked at whether they had identified any issues, whether they had logged those issues in as they should, whether they had corrective action plans in place, and saw the process that they were following. So that is the answer to that.

Ms. CLARKE. Okay. I am going to yield back, Mr. Chairman.

Thank you for your testimony.

Ms. DALY. Thank you.

Mr. MEEHAN. I thank the gentlelady.

The Chairman now—we will recognize as we do under the rules of the committee those Members in order of their appearance at the time of the gaveling down, and so appropriately, the Chairman now recognizes Mr. Perry, from Pennsylvania.

Mr. PERRY. Thank you, Mr. Chairman.

Thank you folks for coming to testify. I must tell you that every single one of you with all due candor, your testimony is breathtaking in concern for me, and I think most Americans, and I imagine other Members of the panel.

That having been said, I am not even sure. Maybe Mr. Salo, you can, I will direct my question to you, but just, I am not sure who should field this, but, you know, I think Americans and Members of Congress are concerned about the navigators.

This is a new position for most people and we don't know exactly what it is going to be like going to a navigator, but we have heard about some of their training.

It is my understanding that they will receive 20 hours of training. I just think about that in the context of the information that these—folks they will be helping us as consumers decide what insurance is best and how to enroll and while right now Members of Congress in our offices cannot advise the public on questions.

We can't do that right now but these folks are going to do that with 20 hours of training and I just want to alert you to the fact that in Pennsylvania—I don't know about other States—but in Pennsylvania, it takes 1,250 hours to become a barber.

All right, it takes a massage therapist 500 hours, and if you want to get a driver's license in Pennsylvania, you have to have 65 hours on the road.

But to navigate insurance for which has been—this thing has been on-going for a couple of years now and Members of Congress and the whole Federal Government can't seem to get information out, these folks are going to be advising us with 20 hours.

So with that, I am wondering, why—it was my understanding first of all, that it was originally 30 hours. Can you verify, can anybody verify that, and if so, why was it cut?

Okay, nobody can verify that.

These folks are, I guess, in that 20 hours—can anybody tell me what training these folks, navigators are going to perceive regarding the security of personal information?

Okay, so—not that—necessarily that you should be able to answer those questions. You know, this is going to range from Social Security numbers to if a woman is pregnant or not. Various organizations which include these individuals are going to be contracted to do this.

Let's just pick one. I know it is somewhat inflammatory, but one would be Planned Parenthood. With the issue of pregnancy being one of the questions being asked, is there some safeguard? Is there some safeguard which offers consumers some kind of recourse?

Let's say that you know, in the information that is gleaned, the woman is pregnant and then this organization, any organization uses that information to advertise to this person their services. Is that appropriate? Is that allowed? What is the recourse? Can anybody provide any information? Okay.

Let me ask you this. With regard to—and this is to Ms. Daly. Thank you very much. According to your testimony, you did not review the functionality of the hub or issues specific to the Privacy Act, but there is an independent—is it my understanding, there is an independent contractor that is going to be doing that or that is doing that currently?

Ms. DALY. That is correct, Congressman. An independent contractor was supposed to be doing this security assessment that would cover over all issues related to security.

With that though, that is supposed to have already been done because it is supposed to be a critical part of the systems authorization that was just recently provided on September 6.

Mr. PERRY. So if that is done, is that information available? The outcomes so to speak or the report on that?

Ms. DALY. I don't believe that is generally available to the public, sir, just because of the sensitivity surrounding that because it

would show what was tested, how the system is configured, things of that nature.

Mr. PERRY. Well, would it—is there some report that will inform the public and Congress, Members of Congress, the Federal Government, regarding the efficacy of that testing and the results? Is this system ready? Is it not?

If it is not, because it is my understanding that the final testing for some of this stuff happens at the end of this month and it is supposed to go live the first of the next month, so we are 20 days away or thereabout, what is the plan or do you know of a plan if it fails?

Ms. DALY. Well, sir, that is a very good point, and I just want to clarify that the testing I've been talking about focused on security aspects of the system, not on the functionality or efficacy of the system.

So that was beyond our scope, so we didn't focus on that because as I mentioned earlier, we were coordinating with GAO and we understood that GAO was going to cover those aspects.

Mr. PERRY. But it is my understanding that the private contractor will be assessing those other milestones so to speak or efficacy. Is that your understanding or don't you know?

Ms. DALY. I honestly can't speak to that, sir. I am sorry.

Mr. PERRY. Can anybody else? One of my—go ahead, Mr. Astrue.

Mr. ASTRUE. I will say one thing. Speaking for myself, I never relied on a contractor to give complete assurance on these things because I mean, no disrespect to this particular contractor, but they are in business to keep the Federal Government contractors happy.

They are not necessarily going to rock the boat. This is why an independent—this is exactly what Offices of Inspector General are set up to do is to make independent assessments about, you know, violations of legal rights, openness to fraud, these types of things.

I am outraged that you would rely on any—I mean, MITRE is a terrific corporation, but I would never rely on MITRE, and I didn't when I was going through dozens of these kinds of programs at SSA.

Mr. PERRY. I have a lot more questions, but I see my time has expired.

I yield back. Thank you.

Thank you, folks.

Mr. MEEHAN. I thank the gentleman.

The Chairman now recognizes the gentleman from Nevada, Mr. Horsford.

Mr. HORSFORD. Thank you, Mr. Chairman. I thank you for this session.

I want to start by first asking: There is in fact a private contractor who is doing this software system development on income and eligibility verification? Is that correct? Whoever can answer the question?

Mr. SALO. At both the State and the Federal levels, yes. I am not the expert at the Federal level; I believe there is one contractor who is doing it at the Federal level.

At the State, generally, it is one contractor, but there are a variety of different private entities that have all bid out with the re-

spective States to do this and to do various components of it ranging from eligibility and enrollment to identity-proofing to conductivity with the hub, et cetera.

But yes, these are generally private contractors. To be honest, I wish that the State experience with IT systems vendors was as rosy as Mr. Astrue said that they are all in the business of making them happy. That is not always true for us.

Mr. PARENTE. But there is only one contractor that has responsibility for building the Federal data hub.

Mr. HORSFORD. Now under at least the Health and Human Services Department, the collection of this type of income and eligibility data occurs across many programs currently, today, correct?

Mr. SALO. Yes, that is correct at least with respect to Medicaid. As I referenced earlier, there are a number of different crosswalks that Medicaid has to do every single day for many of the 72 million people who walk in and out of the door whether that is other Federal or State programs they may be eligible for; TANF, food stamps. You can sometimes work on a joint application to make sure that the shared information works there.

For individuals who are dually-eligible for Medicare and Medicaid, you are cross-walking information across those two programs both from a claims system, from a care coordination perspective, from a program integrity perspective.

You know, Medicaid is the payer of last resort, so we tend to look for you know, does an individual have coverage from some other third-party insurance, or even some sort of settlement from a car crash or something?

So we interface with those systems. Like I said in terms of citizenship documentation, we do all of that. We do all of that every day. The program couldn't run if you didn't do all of those things.

You wouldn't want the program to run if you weren't accessing across programs to get that kind of information because if you are doing that without that kind of information, then you are working blind and that is not the way to go.

Mr. HORSFORD. So Mr. Salo, you said in your testimony that it is important that we focus on how to minimize and mitigate the risks that are inherent in the interconnected parts of these systems and how they work.

So my question and the question I hear from the majority of my constituents including the insurance companies, agents, businesses, they just want this to work, and they want Congress to stop playing games and to figure out ways to make the law work better.

This is the same problem that there was under Medicare and Social Security when they were implemented. It is not going to be perfect on Day 1. So my question is: What are some specific recommendations where we can identify the potential risks and mitigate those risks and what are the steps that we need as Members of Congress to do to ensure that we are putting those steps in place?

Mr. SALO. Well, I am sure you will get a lot of input from other members of the panel, but, you know, I would just say that I agree, you know, from our members' perspective, we just want this to work because at the end of the day, it is the citizen, U.S. citizens,

citizens of the State who are impacted and they don't care whose fault it is. If it goes wrong, they are going to blame us.

You know, in terms of trying to make it work well for them, again, I think this type of conversation is and can be very useful as we raise potential issues. You know, are there, you know, contingencies that perhaps we haven't thought of, whether they are security-related or what have you. I think it is important to get those out in the open so we can think about those and plan for those.

In terms of concrete recommendations, you know, the challenge really is, you know, again, we have got States coming at this from 50 different places and, you know, there has been a challenge—there is a challenge in trying to build a system up in terms of time, in terms of money, in terms of bandwidth.

There is a challenge when it comes to the timeliness of Federal guidance, in terms of, you know, what States can expect, what States have to go, because this is all being done with private contractors, you know, you need time to build into a proposal, into a contract, what exactly they are trying to build, and if you don't know until the last minute, it is really hard to sort-of build that out quickly.

So, you know, the extent to which transparency of information from the Federal perspective comes out in a quicker, more clear way, that would be helpful. I could go on, but I don't want to take up too much time.

Mr. ASTRUE. If I could add for just a few moments. Transparency, as my colleague has pointed out, is important and it is also important as the OIG said that these security documents not be fully public.

I agree with that, but there is a difference in terms of transparency with you and you need to know whether the system is secure, whether it is violating privacy, whether it is doing its job, and you don't know that right now.

If the inspector general defines its job so that those things aren't relevant areas, you need to go to GAO and you need to say to them, "You need to fill the gap where the inspector general is not fulfilling its responsibilities." I believe that the Senate has started to do that.

Mr. HORSFORD. Thank you, Mr. Chairman.

Mr. MEEHAN. Does the gentleman yield back? Oh, okay. I don't want to assume anything. I am just—okay, thank you.

At this point in time, the Chairman now recognizes the gentleman, Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman.

Ms. Daly, based on your testimony, it seems to me that the issue isn't when, or if, but when we are going to have a breach of the data hub or it is going to be leaked or some other problem.

My question is: Has the IG's office developed standards by which a breach such as that would have to be reported to you?

Ms. DALY. Well, Congressman Rogers, the NIST also guides this area in which breaches are reported. There are, you know, certain ways that information needs to be reported, it has to be reported within a certain—

Mr. ROGERS. So you don't have to come in afterwards and audit to find out about it, they have to notify you when they realize there has been a breach or a leak?

Ms. DALY. That is exactly right. They don't notify our office actually, they notify the CIO's office. That is who is responsible for managing that.

Mr. ROGERS. Are they also required to notify the individual whose information was leaked or breached?

Ms. DALY. Well, it depends on if a true breach occurs. First, there is an assessment that is done of it determining the amount of encryption that might have been over the data, and if it is a high enough level of encryption, the individual does not need to be notified.

If there is a certain amount of, you know, risk involved with it and that is a determination that is made in the CIO's office, then the individual of course is notified.

Mr. ROGERS. What about consequences for the navigators, the workers or navigators? If we find one of them has intentionally leaked or breached the security, are there criminal penalties of that you are aware of built into the law or regulations?

Ms. DALY. Well, unfortunately, sir, I am not in a position to answer that today.

Mr. ROGERS. Anybody else on the panel?

Mr. ASTRUE. Yes, there should be an array of—it depends on the nature of the offense, but there should be an array of Federal and State penalties.

Mr. ROGERS. That would already be in existence regardless?

Mr. ASTRUE. It wouldn't—not to say that it might not help for Congress to clarify on that, but there would be existing tools for enforcement if HHS chose to use them.

Mr. ROGERS. Great. This question would be for Mr. Salo or Mr. Astrue.

I have got here a letter signed by 10 State attorneys general, Alabama as being one of them, to Kathleen Sebelius last month and among the questions—they asked several questions they would like clarification on, but among the questions they ask is—and this, I think about Medicaid when I think about this since the State is so heavily involved in it is what is the State's legal liability in this new endeavor if there is a breach? Do either one of you know?

Mr. ASTRUE. Well, with the qualification that I gave up my law license a few years ago, I think generally on these matters—

Mr. ROGERS. Voluntarily?

Mr. ASTRUE. Yes, I did. I did.

Mr. ROGERS. Just joking.

[Laughter.]

Mr. ASTRUE. No, actually, I was afraid as a head of a Government agency I was going to get sued individually, people would go after my bar license, and I decided to give it up.

Mr. ROGERS. I am a recovering attorney myself.

Mr. ASTRUE. Yes. I think as a general matter, this statute, whatever else you might say about it is a classic example of a statute that preempts a lot of State laws. In fact, that has been part of the challenge to the validity of the statute in the first place.

So I think while I would not want to say that there might not be some liabilities for States depending on how much discretion they were using implementing the act, my personal view would be that most of the activities because they are being required by the Federal Government would give the State some immunity from suit.

Mr. ROGERS. Well, it just concerns me that 10 State attorneys general collectively, legally can't discern whether or not they have that liability and one of the things they ask in the letter is do they have or do their respective States have the legal capacity or obligation to add to or supplement the criteria by which this system is operated to make sure they don't have legal liability. Do you know if the States will have that latitude to supplement the security criteria?

Mr. ASTRUE. I think certainly for some features of the act they will have ability to do add-ons. I believe it was designed with, I mean, it is tough to tell from the statute, but it does appear that to me, that it was designed with that intent, and certainly to the extent that you are going beyond the Federal mandate in a discretionary way, it does seem to me that you would be running some risk of losing the protection of the Federal preemption.

Mr. ROGERS. Great. My time is expired.

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

Mr. MEEHAN. Does the Ranking Member have a request?

Ms. CLARKE. Yes, Mr. Chairman. I have a request that the committee—a request for unanimous consent to have Congresswoman Sheila Jackson Lee of Texas sit in and make a comment during our proceedings today.

Mr. MEEHAN. Without objection, so ordered.

Consistent with the rules of the committee, those Members of the committee who are present will take precedence over those who join us.

So I know the gentlelady will yield while we turn to the former U.S. attorney from Pennsylvania, Mr. Marino, for his questioning.

Mr. MARINO. Thank you, Chairman.

Good afternoon, and thank you, folks, for being here today.

Ms. Daly, you have some tough questions that you answered and you are between the devil and the deep blue sea here because of what the AIG technically is supposed to do but based on the lack of information that you may have.

So my question to you is: How can security authorization be made without assurances to you as the IG, that the system itself is secure? Could you explain that to me please?

Ms. DALY. Well, thank you for the question, Congressman Marino.

As part of the NIST guidelines for developing systems, rolling them out, what are the best practices agencies should be following, that is what we have looked at with regards to security for the data hub.

As part of that process, the agencies are supposed to be doing some, you know, continuous testing as it is developed that looks at security and other things too, but our focus was on security, and then at the end, once they get everything developed, they are supposed to have an independent security assessment. That is critical.

Mr. MARINO. But your assessment then is based on the information that you are provided. Correct?

Ms. DALY. That is correct, sir.

Mr. MARINO. You are not making any leaps of faith or conjectures beyond at that point? You are not determining any what-ifs?

Ms. DALY. That is correct, sir. Yes, we basically are reporting out facts in this case. If we had seen something that was a significant violation in any way, we certainly would have reported that and made a recommendation that things be fixed.

Mr. MARINO. Based on what you received.

Ms. DALY. Exactly.

Mr. MARINO. It is like a computer, whatever you put in is the only thing you are going to get out of it. So the only information you get, you based your assessment on what you are given?

Ms. DALY. That is correct, sir. We compared what the testing and the system development documents showed compared to the standards that were in place at that time for that purpose.

Mr. MARINO. This is interesting. I got a phone call from a constituent who works for the State and that person has an insurance health program paid for in part by the State. So that person went to the Social Security Office and because he wanted to get information about Medicare because of the age; 64, 65.

That person asked why I needed to sign up. As that person explained, "I already have insurance, I don't need it. It is being paid for. Why put the taxpayers to an extra cost of now the Federal Government paying and my employer coming in second?"

The answer the clerk gave him was that, "We need this to track you and to garner information about you."

Okay, now, I found that kind of odd. He said, "Well, I only want to sign up for Part A of this," and he again told her that he had insurance and she told him that he would be charged the penalty if he signed up later but the Government needed a system whereby—needed information whereby to track him so they could have information on him to see if he is paying for insurance or has insurance.

Can anyone address this for me? Because I am at quandary as to why.

Mr. ASTRUE. Mr. Marino, with all due respect to my former employee, I don't think that that is an accurate description. My recollection, which is a little soft on the edges is that there was a policy decision made in the late 1960s to link the two together in this way.

It has been litigated. I don't think the rationale of HEW at that time is 100 percent clear. It was litigated fairly recently and I remember being consulted on that litigation a couple of times within the administration in 2007, 2008.

I don't remember when the case was decided. I think it was about 2010, but the decision was that the agency had appropriately linked those two programs together.

But again, I don't think the rationale for why was ever particularly—I think it was lost in the midst of time by the time it got litigated, but I don't think that my former employee's description is probably accurate.

Mr. MARINO. Okay. Mr. Astrue, since we are talking here, can you give me—I know you can go on for a while here, but I only actually have—no, actually, I am over my time, but if you could give us a little synopsis of your opinion of the IG report; pro and con.

Mr. ASTRUE. Yes, I am extremely negative. I think that essentially what happened here is this is not according to GAAP principles.

Essentially, they went in, said, “How are you doing?” And they said, “Well, we are running behind, but we are doing great.” And they said, “Can we see all of the relevant documents?” And they said, “No.”

If you go and read through the report carefully, you will see that the security plan was due on July 15 and there is nothing in the report that says that it wasn’t done on July 15, and this is an August 2 report.

There must have been a draft at that point and I am just not used to the idea that the inspector general comes in and asks for things and you say no. I logged years in the agency and I can’t remember that happening.

So this is a new IG. This is a new IG that is failing in its duty to the American people to dig into what is happening and give answers to the Congress and the American people. I think it is really sad.

Mr. MARINO. Thank you. I yield back my over-spent time.

Mr. MEEHAN. I thank the gentleman, and the Chairman now recognizes the gentlelady from Texas who we are happy to have joined us on the panel today for 5 minutes.

Ms. JACKSON LEE. I thank the gentleman and the Ranking Member for their courtesies, and I think I have some pointed 2 or 3 questions and then a brief comment.

I just always believe the importance of oversight and fact-finding, and I wanted to ask Mr. Astrue, has he engaged our present inspector general in a one-on-one conversation or viewed his documents before your testimony was prepared?

Mr. ASTRUE. No, I have not.

Ms. JACKSON LEE. Then I guess the follow-up is you have first-hand knowledge of what might be some fractures in the structure of exchanges presently being constructed.

Mr. ASTRUE. I had first-hand knowledge through, to some extent, through February of this year, yes.

Ms. JACKSON LEE. In what capacity?

Mr. ASTRUE. As commissioner of Social Security.

Ms. JACKSON LEE. Had the infrastructure of the exchanges begun and to what extent?

Mr. ASTRUE. They had begun since at that point in time, but there was a still a great deal of fluidity in it which for me was the source of considerable concern because the time at that point was really, in my opinion, already too short to do the job properly.

Ms. JACKSON LEE. But that was an opinion? Wasn’t it?

Mr. ASTRUE. Yes, indeed.

Ms. JACKSON LEE. It was February 2013?

Mr. ASTRUE. I left office on February 13, 2013.

Ms. JACKSON LEE. But of this year or last year?

Mr. ASTRUE. This year.

Ms. JACKSON LEE. Yes. So we are now in September.

Mr. ASTRUE. That is right.

Ms. JACKSON LEE. So you are reflecting on the first-hand knowledge that took you up to February and not much further than that. Let's—I thank you for that.

Let me just go to Mr. Salo. National Association of Medicaid Directors, and I am sorry that I missed the explanation of that, but let me go right to the crux of where we are. We all should be concerned about personal information.

However, I think the magnitude of the Affordable Care Act and its overall impact on health care in America is an enormous step forward for saving lives in America.

What would be—do you think we are in the mouth of a whale? Are we about to be swallowed or are we moving forward with the appreciation and respect for personal data as you can see it from your perspective?

Mr. SALO. Oh, I think there has been a very, very long-standing and very, very serious commitment to personal data on behalf of Medicaid, on behalf of the Medicaid directors. They know full well what happens if there is a security breach, and it something that nobody wants.

There are contingency plans. There is constant work being done with chief information officers, with the State IGs, with security experts all the time in Medicaid.

I think the thing to keep in mind about the big picture here, you know, whether we are talking about being swallowed by whales or not, is that security and privacy of data is always a concern, but the thing that has changed is the increasingly interconnected nature of not just our health care system but our overall lives in general.

You know, I am not an expert in banking or credit cards or internet service providers. There are challenges there. The challenges in health care have changed.

You know, we used to store information in unlocked file cabinets in the back of somebody's office. Was that secure? No, it wasn't. So you had to put in place procedures. We have decided as a society, I think rightfully so, that that is not where we want to be and what we need for a variety of reasons is to have much more fluid interconnection of data electronically; whether it is claims or insurance information or what have you.

This is a good thing. It does bring with it different challenges to secure privacy. Not insurmountable ones, different ones. So we adapt accordingly. So I would just see what we are looking at here, whether it is dealing with the Federal hub or what have you, is an outgrowth of that natural progression of how do we figure out how best to secure this information in this inevitable changing world.

Ms. JACKSON LEE. My time is ending, I just want one simple question. Is this any reason to stop moving forward on the Affordable Care Act processes that have been put in place by the Congress and by Health and Human Services?

Mr. SALO. To the best of my knowledge, we will not have security breaches—

Ms. JACKSON LEE. But this is no reason not to go forward?

Mr. SALO. That is correct.

Ms. JACKSON LEE. Thank you.

Let me thank my colleagues and to say that this is an important hearing, and I also think the issue of affordable care is crucial and I think that we are where we need to be, we just need to be particularly more cautious, and I think we can all work together to do that.

Let me yield back. Thank you so very much.

Mr. MEEHAN. I thank the gentlelady for taking the time to join us here today. Let me—I have a few follow-up questions that I would like to pursue. So I recognize myself again for 5 minutes.

Let me just—Dr. Parente, you made some observations in your testimony and I don't want to just leave them hanging out there. You are an expert in dealing with health care databases, you worked intimately in these in the past. You opined in your testimony about concerns of not understanding how the system would work and the potential for fraud. Would you please elaborate on that?

Mr. PARENTE. I will even go further and say most of what I have heard today has not reassured me for several reasons. The first is I have worked, myself, as an independent verification and validation contractor for some Federal databases, actually one in the State of Maryland when Maryland took a step in the 1990s to put together an all-payer database, one of the first in the Nation.

I worked at the time with the Delmarva Medical Foundation and where I worked at Project Hope to essentially be that independent verification and validation contractor and there was a public report and because the Maryland State legislature required it.

I personally find it unconscionable that this contractor, whoever it is, is not at least going to have an executive summary that actually talks about by efficacy the performance standards that would be essentially the safeguards that have been put in for vulnerability tests for the white-hat types of operations that are supposed to be put into place to make sure that all potential compromises have been taken into consideration.

Mr. MEEHAN. Those would be the kinds of things that the certifying officer would have to not only look at but review and rely on. Isn't that right?

Mr. PARENTE. Absolutely, and when I took that roll-on for the State of Maryland, it was a 1-year contract. When I entered and went to look at those databases, worked with other contractors to look at them at different State sites because there were several different vendors involved, and that is one small State, let alone the scale and enormity of what we are discussing today.

Mr. MEEHAN. Well, in light of that, and that is one of the concerns because we talked about the scope and scale of this—Mr. Astrue, you as well, and again, I know that we are asking only for your opinion and not the kinds of asking statements of fact, but I do appreciate once again your testimony touched on something rather significant and you discussed that there was a period of time in which you believed that the HHS may have backed away from its obligations under the Privacy Act and potentially even in violation of the law. Can you articulate? Did I get that correctly and would you say what you mean?

Mr. ASTRUE. Yes, no, and there is a process for this in both—and the IRS came to the same conclusion at about the same time—so we both filed. OMB is the arbiter on those cases and they stalled for a very long time because HHS really didn't have very much to say on the Privacy Act issues.

So it sat for months and months and months. It was not resolved at the time that I left and at some point subsequently I understand they decided that all these issues were under the routine-use exception, but I think that is a real abuse of routine use.

You know, whether you believe in the Affordable Care Act or not, you in the Congress wrote the Privacy Act. You imposed criminal penalties for violations of the Privacy Act and so those of us who are in the Executive branch or were in the Executive branch, we are supposed to be respecting that. I found the HHS disregard for the Privacy Act to be really shocking.

Mr. MEEHAN. Let's pursue that for a second. Again, as a former prosecutor, I am concerned about this issue of routine use and, for the record, routine use is, "a disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."

So anything beyond that would be a violation of routine use. So we are already beginning to collect information that relies to some database and then there is a broad, broad expansion of how information originally collected is going to be utilized. Is that not accurate?

Mr. ASTRUE. Yes, that is correct.

Mr. MEEHAN. Okay, so even if there is an interpretation with regard to that within routine use because it is all part of a hub and it is used as verification, one of the great concerns I have has been the derivative use of information that is being gathered by navigators.

So where we have navigators who are going to be asking personally identifying information, do we have any checks on whether or not they will have any other kind of use except for the sole purpose, the entire sole purpose of facilitating activities on the exchange?

Mr. ASTRUE. No, I think that is a fine point. You, Mr. Chairman, and other Members of the committee earlier pointed out that these are not even typical Americans. These are disproportionately disadvantaged Americans in some of our most vulnerable populations.

To send navigators out with a minimum of training, no background checks in many instances, that is an invitation for fraud. I have spent—I have been working on fraud against the elderly since 1979 off and on in my career, and I just shudder at the thought of untrained people, unsupervised by, in any substantial way by HHS, going out with no real monitoring or accountability systems saying, "Hi, I am here from the Federal Government. Let's talk about some of the most intimate choices you need to do, and you need to apply for this, and by the way, what is your Social Security number?"

I mean, that is exactly the thing that the inspector general should be screaming bloody murder about because if that is not an invitation to widespread fraud against our most vulnerable people in this country, I don't know what is.

Mr. MEEHAN. Are you aware of whether or not there is, within this, the requirement that there be background checks for any individual who is going to serve as a navigator?

Mr. ASTRUE. My understanding is that many of these people are being hired without background checks.

Mr. MEEHAN. So somebody could be actually convicted of identity theft and then become a navigator?

Mr. ASTRUE. I think you need to ask—

Mr. MEEHAN. Mr. Salo, is that accurate? Are you doing background checks on anybody that you are familiar with?

Mr. SALO. Navigators aren't actually a Medicaid function so we are not directly involved in the hiring of them so I can't speak to whether or not there are adequate background checks or other securities there.

Mr. MEEHAN. Mr. Astrue, let me just ask one other question again because I am trying to create a record because I want to see what is going to happen at some future time, and the bottom line is again because we can foresee the potential for utilization of information that is beyond the scope of even an interpretation of what would routine use be and we have now identified.

Now those people who have certified the stability of this system in light of the recognition that those are potential things here, willful acts of the privacy, the Federal Government itself, and I have the case law that supports it.

It is a willful—it is the—imposes liability on the agency when they violate the Privacy Act by willful or an intentional matter either by committing the act without grounds for believing it to be lawful or flagrantly disregarding other's rights under the Act.

Mr. ASTRUE. That is exactly right and the issue first came to my attention, and I know I talked to a *Washington Post* reporter last night who was quite sure that everything I said was horribly political and ideological, but this issue first came to my attention because my own civil servants who would be doing this came to me and said, "I am afraid I am going to be prosecuted for doing this."

Mr. MEEHAN. Wouldn't it be prudent and do you believe that the standard of responsibility is such that before certifying it there would be checks to assure that people with criminal records would not have access to personally identifying information of individuals who were going to be signed on to the exchange?

Mr. ASTRUE. Absolutely. They are going to be asking for extraordinarily sensitive information in many cases including—it is just a Social Security number. You know, people can run wild and destroy someone's life, you know, taking a Social Security number. It is a big problem in our society.

Mr. MEEHAN. My time has expired.

I now ask the Ranking Member if she has follow-up questions.

Ms. CLARKE. I do, Mr. Chairman.

I would like to follow up with Mr. Salo. Your testimony mentions all of the ways in which States and State Medicaid programs already work with a variety of public and private data systems. State Medicaid programs already communicate with Federal agencies to verify citizenship. Isn't that correct?

Mr. SALO. That is correct.

Ms. CLARKE. They may communicate with other programs like TANF and SNAP as well?

Mr. SALO. Correct.

Ms. CLARKE. They also communicate with private entities like private insurance companies, right?

Mr. SALO. Correct.

Ms. CLARKE. Is it correct for me to assume that data that is transmitted is personally identifiable?

Mr. SALO. In many cases, yes it is. Not always, but if it needs to be, it is.

Ms. CLARKE. So State Medicaid programs across the country have for years exchanged personally identifiable data with Federal and private data systems. We know that any data system can be susceptible to a breach, but have State Medicaid programs experienced any program beyond of those we see in the data systems of private industry?

Mr. SALO. No.

Ms. CLARKE. So could State Medicaid programs function without this ability to share and retrieve data from other systems?

Mr. SALO. No, and I don't think we would want it to.

Ms. CLARKE. You have described a heavy lift for States, but also a good partnership with the Federal Government to get this accomplished. It is my understanding that HHS has made a 90:10 matching rate available for upgrades to States' eligibility and enrollment systems regardless of whether a State chooses to expand.

Can you comment on the number of States that have availed themselves of this funding?

Mr. SALO. Yes, my understanding is that literally every State has availed itself of that funding. There were certainly some examples of States that had turned back other specific funding for, call it early innovator grants, but in terms of the money that it took and that it is taking to update, to upgrade, to transform the current Medicaid eligibility systems, many of which are legacy systems that go back unfortunately to the 1980s, every State has availed itself of the 90:10 funding.

The question then actually is: Is 90:10 enough? The question is: Even with that, even if there were enough funding, is there enough time to make those changes? Is there the bandwidth within the IT systems vendor community?

You know, I often used to joke that when we look at the history of Medicaid and systems changes, the number of times that you got a contract in on time, on budget, and to spec was, well three times in the history of Medicaid.

[Laughter.]

Mr. SALO. So, a lot of people, I think myself included would argue you just need to do something very, very different here. But having said that, in the run-up to October 1, and in the time soon thereafter, the States and the Feds and the IT systems vendors have worked double, triple, quadruple overtime to make this work.

So we do believe the system will be up and running come October 1. As I said, it will be bumpy. The consumer experience will not be a smooth and seamless Travelocity, but it will be a system in place that with workarounds, with, you know, having contingency plans going back to using paper, going into the Medicaid office,

what have you, insurance and subsidies, and that will be available, and it is our goal, it is our plan over the next couple of months to make sure that we improve that as we go.

Ms. CLARKE. I would agree with you. So much of our information is in the public and private domain that, you know, I think we need to take a step back and give this an opportunity to rollout and work with it to make sure that the American people get the very best access to health insurance that they possibly can.

I mean, just about every American has had an opportunity to go on-line and to provide information and you know, we don't have the most secure, unbreachable IT operations in our own homes and families.

So to sort of prejudice just how secure this process will be, will be pretty relative to the security of our IT systems, Nation-wide, the ones that we use each and every day whether it is to pay a phone bill, whether it is to purchase something on-line.

I am concerned that we not create a panic around the situation but that we give it our best efforts in terms of providing an opportunity to make this thing work and to work out the kinks as we go along.

There are going to be kinks. We all know that. There is not one system that I know of that has been perfect. People have bought iPhones and they have been, you know, breachable right out of the box. So, you know, let's not sit here and act as though we have perfection on our side.

Personal information is critical and its security is critical to all of us, but at the same time we have managed given the massive use of IT systems around this Nation to keep breaches to a minimum given the number of people and transactions that take place each and every day.

With that, Mr. Chairman, I yield back.

Mr. MEEHAN. Well I want to thank the gentlelady for yielding back.

I want to thank each of the witnesses for your testimony here today. I am grateful and I appreciate, with the exception of Ms. Daly, each and every one of you effectively don't have to be here, that you were responsive to our inquiries, and I am grateful for your taking the time using your professional expertise to help us better understand a situation in which it is still my considered opinion that this hearing has demonstrated by virtue of testimony even more questions about the readiness.

There has been testimony as said it is not a question that this needs to be a stepping-off point to prevent a system from being put in place, but is it ready to go today?

At a certain point, is it so clear that it is not ready that the requirements that are continuing to push this forward at a certain point start to become perhaps not even just negligent, but otherwise. Great concern to me.

Once again, I want to thank each of the panelists for their valuable testimony.

Well, I am not getting ready to close because the Member from Pennsylvania has one final question.

Mr. MARINO. Thank you. I refer to my prosecutorial background as the Chairman does. We were U.S. attorneys together, but I want to bring up two points if I may.

Mr. Astrue, you were questioned about when you left the agency, and I think it was pointed out that you hadn't been there in, what would it be now, 9 months or 8 months. How long were you with the agency before that?

Mr. ASTRUE. Six years and a day.

Mr. MARINO. You based your opinion on your experience over that 6-year period and what you had gleaned even before that in your career.

Mr. ASTRUE. Sure, and since that time, I have tried to keep up on the issue. I don't call into the agency, but people retire, you talk to people—

Mr. MARINO. Well, we do call into the agency and ask because we get calls from our constituents, "What do I do about this?" "What do I do about that?"

Since last year up until September, and I get the same answers now in September that I did last year and in January and February of this year is "We don't know." So given the fact that there have been waivers, delays, I don't think much has changed over the last 1.5 to 2 years.

In conclusion, ma'am, could you please tell me, did you ever have a point when you were doing these investigations concerning security that you thought maybe a statement should have been made to HHS, Health and Human Services, HHS concerning I don't have enough data to form an opinion as to what the security is going to be or not be?

Ms. DALY. Well, Congressman, I want to focus—initially, on the scope of our work, the scope of our work really wasn't to provide an opinion. We were actually going out there to do just an audit over that. We were provided the data that we had requested if it was, even had been created.

That is one of the challenges. I have done a number of system development jobs over my career of a variety of systems and it is always a challenge when you are doing this because you are doing something that doesn't exist yet and so that makes it more challenging to get all of the information—

Mr. MARINO. Good point. I mean, did you ever raise that? These things do not exist yet, so how can we form a conclusion, a factual conclusion?

Ms. DALY. Well, that is exactly right. So in those cases, that is why we reported that the information wasn't available and when they expected to have it available. That is clearly what was in our report.

If you could beg me an indulgence, I would like to say that I think our office of inspector general is one of the most highly-respected in the accountability community and that we do a tremendous job for the American citizen and taxpayer.

Our office returned \$6.9 billion in expected recoveries last year along with over 1,100 civil and criminal actions, and I think our record speaks for itself. Thank you.

Mr. MARINO. We rely on you.

Ms. DALY. Thank you. Thank you.

Mr. MARINO. We rely on you.

Again, thank you so much.

Chairman, thank you so much for indulging me.

Mr. MEEHAN. Thank you.

Ms. Daly, I do thank you for your service.

I thank each of the panelists. The Members of the committee may have some additional questions for the witnesses, and if they are directed to you I would ask that if you can, you would respond in writing.

So without objection, the committee, the subcommittee now stands adjourned.

[Whereupon, at 4:32 p.m., the subcommittee was adjourned.]

