AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY: THE DEPARTMENT OF THE INTERIOR

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

AND THE

SUBCOMMITTEE ON THE INTERIOR

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JULY 15, 2015

Serial No. 114–52

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

97–789 PDF WASHINGTON : 2016

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DeSAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
WILLIAM MCGRATH, *Interior Subcommittee Staff Director*
TROY STOCK, *IT Subcommittee Staff Director*
MELISSA BEAUMONT, *Clerk*

Subcommittee on Information Technology

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALLER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

Subcommittee on the Interior

Cynthia M. Lummis, Wyoming, *Chairman*

KEN BUCK, Colorado, *Vice Chair*
PAUL A. GOSAR, Arizona
BLAKE FARENTHOLD, Texas
STEVE RUSSELL, Oklahoma
GARY J. PALMER, Alabama

BRENDA L. LAWRENCE, Michigan, *Ranking Member*
MATT CARTWRIGHT, Pennsylvania
STACEY E. PLASKETT, Virgin Islands

CONTENTS

	Page
Hearing held on July 15, 2015	1

WITNESSES

Ms. Sylvia Burns, Chief Information Officer, U.S. Department of the Interior	
Oral Statement	4
Written Statement	7
Ms. Mary Kendall, Deputy Inspector General, U.S. Department of the Interior	
Oral Statement	11
Written Statement	13

APPENDIX

Office of Personnel Management Mission Statement, submitted by Rep. Lieu	40
July 9, 2015 Dept. of the Interior Response to the Office of the Inspector General Report, submitted by Chairman Hurd	42
Nov. 26, 2013 Dept. of the Interior, Office of the Inspector General Report on Faisal Ahmed, submitted by Chairman Hurd	51
Colleen M. Kelley, National President, Statement of the National Treasury Employees Union, submitted by Chairman Hurd	54
Statement of Congressman Gerald E. Connolly (VA–11), submitted by Chairman Hurd	57
Office of the Inspector General, U.S. Department of the Interior Report: Security of the U.S. Department of the Interior's Publicly Accessible Information Tehnology Systems, submitted by Chairman Hurd	59

CYBERSECURITY: THE DEPARTMENT OF THE INTERIOR

Wednesday, July 15, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY, JOINT
WITH THE SUBCOMMITTEE ON THE INTERIOR,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:38 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present from Subcommittee on Information Technology: Representatives Hurd, Farenthold, Blum, Kelly, and Lieu.

Present from Subcommittee on the Interior: Representatives Lummis, Russell, Palmer, Lawrence, and Cartwright.

Mr. HURD. The Subcommittee on Information Technology and the Subcommittee on the Interior will come to order. And, without objection, the chair is authorized to declare a recess at any time.

Good afternoon. Thanks for being here today. Sorry for the delay. You all know how it is here in Washington. This is an important hearing. In the wake of the data breach of the Office of Personnel Management, the committee remains deeply concerned with the Federal Government's plan to address cybersecurity. This do as I say, not as I do mentality is an affront to the American people and leaves our Federal agencies and the PII of millions at risk.

Today's hearing is the first in a series of hearings the Subcommittee on Information Technology will hold to focus on the cybersecurity posture of Federal agencies. This means not only compliance with FISMA, but also responding to the recommendation from an agency's inspector general, as well the GAO.

I'm proud to hold this hearing jointly with Chairwoman Lummis, Ranking Member Lawrence, and the Subcommittee of Interior. And I am always thankful for Ranking Member Kelly and the bipartisan way we have been able to approach cybersecurity and other issues on this subcommittee.

The first hearing this committee held on the recent OPM data breach I advised agency CIOs across the Federal Government to pull out their past IG reports and get to work on addressing the vulnerabilities that have been identified.

Ms. Burns, I hope you have come here today with a concrete plan to address vulnerabilities in DOI's systems pointed out by the IG and others.

The Department of Interior inspector general recently conducted penetration tests of publicly accessible computer systems and Web

sites operated by DOI bureaus. What they found is alarming and is largely what brings us here today. The IG found nearly 3,000 critical and high-risk vulnerabilities in hundreds of publicly accessible computers operated by DOI bureaus. Let me repeat that number: 3,000.

Even more concerning, the IG found that because DOI did not segment its publicly accessible systems from its internal systems, hackers could exploit these vulnerabilities to access internal or nonpublic DOI computer networks. DOI's internal networks support mission-critical operation and contain highly sensitive data. Not segmenting the public and the internal networks from each other is a failure of basic cybersecurity best practices.

We need and deserve better from Federal agencies and those in charge of securing our digital assets. There's too much at risk not to.

In addition, DOI hosted the OPM personnel file database that was breached and resulted in 4.2 million former and current Federal employees having their personal and private information stolen. Since then, Director Archuleta has stepped down and rightfully so.

Several questions about DOI's role in the breach remain unanswered, including whether or not other agencies may have been compromised, how many breaches exactly took place at DOI, and whether or not the attackers are still in the system. Both subcommittees look forward today to having some of those questions answered.

In closing, it is no secret that Federal agencies have a long way to go to improve their cybersecurity posture. We have years and years of reports highlighting the vulnerabilities and inactions of Federal agencies. We also have years and years of recommendations from IGs, GAO, and experts in and out of the government on how to address these vulnerabilities. Simply put, we know what needs to be done, we just need to do it.

We need strong and capable leaders in place across the Federal Government to upgrade IT systems and shore up the current sorry state of cybersecurity at Federal agencies. We need leaders who will listen to the recommendations of their IGs and others and take appropriate corrective actions based on those recommendations. The status quo is unacceptable. We need leaders who can put a solid plan in place and then execute it.

I hope we have that type of leadership in place at DOI. I welcome the witnesses and look forward to their testimony.

And now, I'd like to recognize my friend and the ranking member, Ms. Kelly of Illinois.

Ms. KELLY. Thank you, Mr. Chairman, and welcome to the witnesses.

Last month, the Oversight Committee held hearings on two major OPM data breaches. We learned that the stolen personnel records of over 4 million current and former Federal employees were kept on servers hosted by the Department of Interior. Hackers essentially not only gained access to OPM's personal records, but in doing so they successfully penetrated the Department's data center where the records have been stored.

Fortunately, an ongoing investigation into the OPM breach has so far not uncovered any evidence that any of the Department's data was stolen during the time period hackers had access to the data center. But the fact that the Department's computer systems were also hacked raises serious questions about the strength of the Department's cybersecurity system.

Last week, the Department's inspector general provided the general with a draft that identified security weaknesses the IG found in many of the publicly accessible computers the Department maintains. Computers such as these are primarily used by the Department to share information with the public, collaborate with business and research partners, and to provide employees and contractors remote access to Department networks.

As the IG noted in his draft report, and I quote: "Publicly accessible computers operated by Federal agencies are prime targets for exploitation and are highly sought after by criminals and foreign intelligence services."

According to the IG, over the past several years hackers and foreign intelligence services has been able to compromise the Department's computer network by exploiting weaknesses in its publicly accessible system. The IG's draft report provides a clear warning about a serious security vulnerability in the Department's publicly accessible computers.

As I pointed out in my opening remarks at the subcommittee's first hearing this year, no organization is immune from cyber attacks and data breaches. As we saw this past year, sophisticated companies, from Anthem to JPMorgan Chase, were all targeted and breached by cyber attackers.

I do want to acknowledge and thank Chairman Hurd for the bipartisan approach he has taken on the issue of cybersecurity.

Mr. Chairman, I know we can work together to solve this. Thank you, and I yield the balance of my time.

Mr. HURD. Thank you, Ms. Kelly.

And now it is a pleasure to recognize Mrs. Lummis, the chairwoman of the Subcommittee on the Interior, for her opening statement.

Mrs. LUMMIS. Well, thank you, Chairman Hurd, for leading this hearing.

As we know, the Department of the Interior hosted a database for the Office of Personnel Management containing the records of approximately 4.2 million current and former government employees. Now, as we've seen, shared hosting can reduce redundancy and costs for government IT needs. Also as we've seen, however, it can result in increased vulnerability if it's not properly managed.

So in this hearing, I look forward to learning more about the response by Interior to the breach, their compliance with the Federal Information Security Management Act and the Federal Information Technology Acquisition Reform Act, and past and future management decisions regarding recommendations by inspectors general for improving cybersecurity.

So thanks again, Mr. Chairman.

And thank you, witnesses, for being here today.

I yield back.

Mr. HURD. When Mrs. Lawrence, the ranking member of the Subcommittee on the Interior, is here we'll recognize her for her opening remarks. Until that time, I'd like to turn to our witnesses and introduce them. And I'm also going to hold open the record for 5 legislative days for any members who would like to submit a written statement.

Mr. HURD. I'm pleased to welcome Ms. Sylvia Burns, the Chief Information Officer at the U.S. Department of the Interior; Ms. Mary Kendall, Deputy Inspector General at the U.S. Department of the Interior as well.

Welcome to you both.

It is also my understanding that our witnesses are accompanied by two additional experts whose expertise may be needed during questioning. And so I'd like to welcome Mr. Jefferson Gilkeson, Director of IT Audits at the U.S. Department of Interior, and Mr. Bernard Mazer, Senior Policy Advisor in the Office of Inspector General at the U.S. Department of Interior and the former Interior CIO.

Pursuant to committee rules, all witnesses will be sworn in before they testify, including Mr. Gilkeson and Mr. Mazer. So please rise and raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Please be seated.

Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for discussion, please limit your testimony to 5 minutes. Your entire written statements will be made part of the record.

And we're going to start with you Ms. Burns. You're now recognized for 5 minutes for your opening remarks.

WITNESS STATEMENTS

STATEMENT OF SYLVIA BURNS

Ms. BURNS. Chairmen Hurd and Lummis, Ranking Members Kelly and Lawrence, and members of the subcommittee, thank you for the opportunity to discuss cybersecurity at the Department of the Interior. I am Sylvia Burns, and I have been the Department's Chief Information Officer since August 24, 2014.

The Department and its bureaus serve as stewards of the Nation's parks, wildlife refuges, and public lands. And as the keeper of the history of this country, over 70,000 employees in more than 2,400 operating locations, including many remote areas, carry out the Department's mission across the United States and its territories.

The Department is committed to cybersecurity and the protection of our assets, including data. IT tools are of vital importance to the delivery of the mission of the Department. The security of those IT tools and systems is likewise critical to our mission. All levels of our Department are engaged in the efforts to improve our cybersecurity.

My office provides leadership to the Department and its bureaus in all areas of information management and technology. The Department's programs are many and varied. The Department's current IT management and operations structure reflects the decentralized nature of IT programs. My office is responsible for the operation of many departmental systems and issues IT policy, while bureaus and offices are each responsible for their respective systems.

Each week the Department detects and prevents between 5 million and 6 million malicious connection attempts to exploit vulnerabilities in its Internet perimeter and Internet-facing systems. My office is working in partnership with the Department's senior leadership and IT personnel in the bureaus and offices to improve our ability to manage the risk of cyber attacks while delivering the Department's mission.

I recently established a Department-wide cybersecurity advisory group to support me in developing and implementing a comprehensive, multipronged cybersecurity strategy and action plan, which includes short, medium and long-term initiatives to strengthen the Department's IT security posture.

We are in the process of adopting a more centralized approach, managing IT across the Department. For instance, to meet FISMA requirements, the Department will obtain access and visibility into the entire Department network and will play a more direct role in incident response working with its bureaus and office and with US–CERT.

As a result of a secretarial order, FISMA and FITARA, DOI achieve the following. Through the Continuous Diagnostics and Mitigation investment funded by Congress through DHS, DOI deployed capabilities to centrally manage vulnerability patching at the Department level, which will greatly improve cyber hygiene across our IT landscape.

As of June 26, the Department implemented strong authentication for all privileged users. I am happy to report that as of this morning we have achieved 75 percent of PIV enablement for our unprivileged users. That was news.

The Department launched its data center consolidation plan to support the OMB Federal Data Center Consolidation Initiative. Data center consolidation reduces the Department's IT footprint overall, consolidating smaller, noncore data centers into DOI's larger and more robust core data centers, allows us to more efficiently and effectively manage and protect high value data.

The Department supports and appreciates the work of the Office of the Inspector General in assessing and advising the Department on its IT systems. We accept all of the OIG's recommendations and will incorporate them into our action plan. The impacted bureaus report that all vulnerabilities identified in the report have been corrected.

The Department takes the privacy and security of its IT systems and data very seriously. The Department immediately and aggressively responded to the recent cyber intrusion resulting in the loss of OPM data. We worked with interagency partners who are addressing the broader cybersecurity threats to the Federal Government to develop and implement an immediate remediation plan

specific to the threat. We incorporated remediation actions, the OIG's recommendations, and departmental IT improvements which were already underway into the Department's overall IT strategy moving forward.

We will continue to be an active participant in the ongoing efforts by the Federal Government to improve our Nation's overall cybersecurity posture.

Chairmen Hurd and Lummis, Members Kelly and Lawrence, and members of the subcommittee, this concludes my prepared statement. I would be happy to answer any questions you have.

[Prepared statement of Ms. Burns follows:]

STATEMENT OF SYLVIA BURNS
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF THE INTERIOR

BEFORE THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY AND
SUBCOMMITTE ON THE INTERIOR
JULY 15, 2015

Chairmen Hurd and Lummis, Ranking Members Kelly and Lawrence, and Members of the Subcommittees, thank you for the opportunity to discuss cybersecurity at the Department of the Interior ("Department" or "DOI"). I am Sylvia Burns, and have been the Department's Chief Information Officer since August 24, 2014.

The Department and its bureaus serve as stewards of the nation's parks, wildlife refuges, and public lands, and as the keeper of the history of this country. The Department's bureaus oversee the responsible development of U.S. energy resources, supply and manage water in the western states, and maintain relationships and provide services to tribes and native peoples. The Department also delivers science and community-based programs that engage the participation of citizens, groups and businesses. Over 70,000 employees in more than 2,400 operating locations, including many remote areas, carry out the Department's mission serving communities large and small across the United States and its territories.

The Department is committed to cybersecurity and the protection of our assets, including data, infrastructure and our employees. Information technology (IT) tools are of vital importance to the delivery of the mission of the Department. The security of those IT tools and systems is, likewise, critical to our mission. All levels of our Department are engaged in, and supportive of, providing the support and resources necessary to improve our cybersecurity.

The Office of the Chief Information Officer (OCIO) provides leadership to the Department and its bureaus in all areas of information management and technology. To successfully serve the Department's multiple missions, the OCIO applies modern IT tools, approaches, systems and products. Effective and innovative use of technology and information resources enables transparency and accessibility of information and services for the public.

The Department's programs are many and varied. The Department's current IT management and operations structure reflects the decentralized nature of its programs and functions. The OCIO is responsible for the operation of many Departmental systems and issues IT policy, while bureaus and offices are each responsible for their respective systems and local area networks (LANs). The DOI OCIO is also responsible for reporting IT security incidents that we receive from bureaus and offices to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) and for relaying reports from US-CERT to bureaus and

offices for appropriate action. In addition, the Department maintains an Advanced Security Operations Center (ASOC) with advanced tools to monitor network traffic and perimeter activity for the wide area network (WAN), which the bureaus and offices can leverage.

Each week, the Department detects and prevents between five and six million malicious connection attempts to exploit vulnerabilities in its Internet perimeter and Internet facing systems. The OCIO is working in partnership with the Department's senior leadership and IT personnel in the bureaus and offices to improve our ability to manage the risk of cyber-attacks while delivering the Department's mission.

The OCIO recently established a Department-wide cybersecurity advisory group which includes experts from a variety of IT and management disciplines. The group is advising and supporting me in developing and implementing a comprehensive, multi-pronged, cybersecurity strategy and action plan for the agency. This will include short, medium and long-term initiatives to strengthen the Department's IT security posture. In addition, the Department's on-going implementation of Secretarial Order 3309, *Information Technology Management Functions and Establishment of Funding Authorities*, the Federal Information Technology Acquisition Reform Act (FITARA), and the Federal Information Security Modernization Act (FISMA), will address many of the long-standing challenges in IT management.

Pursuant to these initiatives, the Department is in the process of adopting a more centralized approach to managing IT across the Department. For instance, to meet FISMA requirements, the Department will obtain access and visibility into the entire Department network and will play a more direct role in incident response working with its bureaus and offices and with US-CERT.

As a result of Secretarial Order 3309, FISMA and FITARA, DOI achieved the following:

- The Department improved cybersecurity capabilities using the Continuous Diagnostics and Mitigation (CDM) investment funded by Congress through DHS. Through this investment, DOI deployed continuous monitoring capabilities across the enterprise to DOI computing devices, including laptops, desktops, and servers. This gives the Department visibility into the vast majority of IT hardware and software assets on our network. Our CDM tools also give us the opportunity to centrally manage vulnerability patching at the Department level, which will greatly improve cyber hygiene across our IT landscape.

- Based on FISMA requirements, as of June 26, 2015, the Department implemented strong authentication for all privileged users across the Department. Two-factor authentication provides strong controls to ensure that only authorized users, whether a system administrator, or regular end-user, are able to gain access to DOI's IT systems. This protects us from intruders who can compromise usernames and passwords to gain access to our network.

- Recently, the Department successfully consolidated 14 disparate email systems and moved more than 70,000 employees to a single, cloud-based email and collaboration system, known as BisonConnect. We also implemented a separate, but integrated

cloud-based electronic document and records management system to support the electronic journaling of emails. Reducing the number of duplicative email systems with different security policies and configurations helped the Department to shrink the threat surface around our email systems, enforcing a standard that we can more effectively and efficiently secure.

- The Department awarded a set of contracts to support our move to the cloud and recently migrated another major application, the Financial and Business Management System (FBMS), a customized SAP application, to the cloud. To support the Federal CIO's "Cloud First" Strategy, DOI implemented a Mandatory Use Policy for the Foundation Cloud Hosting Services Contract requiring all bureaus and offices to evaluate cloud services first when refreshing technologies or standing up new initiatives. As of July 2015, DOI awarded 15 cloud hosting contract task orders for internal and external customers. This provides the Department access to state-of-the-art, commercial "infrastructure-as-a-service (IAAS), platform-as-a-service (PAAS) and software-as-a-service (SAAS)" offerings that are FedRamp compliant. The cloud provides a flexible, scalable, cost-effective and secure environment for hosting DOI's applications and data. We see the cloud as a pivotal part of our long-term future.

- The Department launched its data center consolidation plan to support the OMB Federal Data Center Consolidation Initiative. Since 2011, we consolidated 127 DOI data centers, exceeding DOI's initial commitment of 95 data centers. In addition, the Department categorized six data centers as core data centers, and will leverage them as internal hosting consolidation points in addition to cloud and third-party options. Data center consolidation reduces the Department's IT footprint overall and provides us with internal hosting options for systems that are not yet cloud-ready. Consolidating smaller, non-core data centers into DOI's larger and more robust core data centers allows us to more efficiently and effectively manage and protect high value data.

The Department supports and appreciates the work of the Office of Inspector General (OIG) in assessing and advising the Department on its information technology systems. We believe that the OIG's *Evaluation Report, Security of the U.S. Department of the Interior's Publicly Accessible Information Technology*, provides valuable information about potential vulnerabilities of the information technology systems to outside intrusions and assists greatly in the Department's ongoing efforts to strengthen data security. Accordingly, the Department and its bureaus fully cooperated with the OIG upon being advised of this assessment.

The Department accepts all of the OIG's recommendations, and will incorporate them into a Departmental cybersecurity action plan. Further, the Department is engaging all bureaus and offices in discussions about the OIG's findings and the need to undertake major changes in how we manage publicly facing systems across the entire Department. The impacted bureaus report the vulnerabilities identified in the report have been corrected.

The Department takes the privacy and security of its IT systems and data very seriously. The Department immediately and aggressively responded to the recent cyber intrusion resulting in the loss of OPM data. We worked with interagency partners, who are addressing the broader

cybersecurity threats to the Federal Government, to develop and implement an immediate remediation plan specific to that threat. We incorporated remediation actions, the OIG's recommendations, and Departmental IT improvements, which were already underway, into the Departments overall IT strategy moving forward. We will continue to be an active participant in the ongoing efforts by the Federal government to improve our nation's overall cybersecurity posture.

Chairmen Hurd and Lummis, Ranking Members Kelly and Lawrence, and Members of the Subcommittees, this concludes my prepared statement. I would be happy to answer any questions that you may have.

Mr. HURD. Thank you, Ms. Burns.

Now over to you, Ms. Kendall, for 5 minutes.

STATEMENT OF MARY KENDALL

Ms. KENDALL. Mr. Chairman, Madam Chairman, Ranking Member Kelly, and members of the subcommittees, good afternoon, and thank you for the opportunity to testify today about the results of our OIG audit on security of public-facing Web sites at the Department of the Interior.

Although the OIG has had an IT oversight function for over a decade, we have refocused our IT oversight efforts over the past 3 years. In 2012, we began to transfer the responsibility for conducting IT oversight to our Office of Audits, Inspections, and Evaluations in order to standardize and track our IT oversight of the Department, and we have since doubled the number of IT professionals assigned to this oversight.

Our focus on IT oversight has evolved over the years from periodic assessments and compliance reporting to using tools and techniques to conduct ongoing monitoring of IT security controls, an approach that enables responsible officials to take timely risk-mitigation actions and make risk-based decisions regarding the operation of their IT systems.

This is how we conducted the IT audit at issue in today's hearing. The results of our efforts provided the bureaus with real-time information necessary for them to take prompt action. A future OIG follow-up audit will determine whether those actions were effective at addressing the vulnerabilities identified.

"Defense in depth" is a widely recognized best practice for protecting critical IT assets from loss or disruption by implementing overlapping security controls. The concept of defense in depth is that if one control fails, then another is in place to either prevent or limit the adverse effect of an inevitable cyber attack.

We found that three DOI bureaus had not implemented effective defense in depth measures to protect key IT assets from Internet-based cyber attacks. We found critical and high-risk vulnerabilities in publicly accessible computers operated by these bureaus. If exploited, these vulnerabilities would allow a remote attacker to take control of publicly accessible computers or render them unavailable.

In addition, we found that a remote attacker could then use a compromised computer to attack the Department's internal networks that host computer systems supporting mission-critical operations and containing highly sensitive data. These deficiencies occurred because the Department did not effectively monitor its publicly accessible systems to ensure they were free of vulnerabilities or isolate its publicly accessible systems from its internal computer networks to limit the potential adverse effects of a successful cyber attack.

The results contained in this report are the first in a series of defense in depth. We made recommendations designed to help the Department mitigate, identify vulnerabilities, and strengthen security practices, reduce the opportunity for a malicious attack, and minimize the impact and potential opportunities to infiltrate nonpublic systems after a successful attack. The Department concurred

with all of our recommendations and has begun to implement them.

We are preparing a public version of our report, but as we continue to analyze the content, we determined that details of our methodology, specifically the "how we did our testing and with what tools," and certain details of the results of our testing, could cause harm to the Department and its IT assets. We will therefore redact this information along with the identity of the bureaus that were subject to our testing in the public version of our final report, which will be posted on our Web site.

As is our practice however, Chairmen Hurd and Lummis, we will be glad to provide you with a copy of our full final report at your request.

Mr. Chairman, Madam Chairman, ranking members, this concludes my prepared remarks today. I am happy to try to answer any questions you or members of the subcommittee may have, but I would also be assisted by Mr. Gilkeson and Mr. Mazer.

[Prepared statement of Ms. Kendall follows:]

TESTIMONY OF MARY L. KENDALL
DEPUTY INSPECTOR GENERAL
FOR THE DEPARTMENT OF THE INTERIOR
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
AND SUBCOMMITTEE ON INTERIOR
UNITED STATES HOUSE OF REPRESENTATIVES
JULY 15, 2015

Mr. Chairman, Madam Chairman, and members of the Subcommittees on Information Technology and Interior. Good afternoon. Thank you for the opportunity to testify today about the results of an Office of Inspector General (OIG) review of security of public-facing websites at the U.S. Department of the Interior (DOI or Department). I am joined today by Jefferson Gilkeson and Bernard Mazer, who are prepared to help answer any technical questions you may have.

IT Security at DOI and OIG Oversight

Although OIG has had an IT oversight function for over a decade, we have refined and refocused our oversight efforts in the past 3 years. In 2012, we began to transfer the responsibility for conducting IT oversight from our Office of Management to our Office of Audits, Inspections, and Evaluations (AIE) in order to standardize and track our IT oversight of the Department. In addition, we have incrementally doubled the number of full-time equivalent employees (FTEs) assigned to IT oversight.

In fiscal year (FY) 2014, OIG conducted IT oversight in areas such as evaluating DOI's security practices for protecting mission-critical IT assets, assessing DOI's cloud-computing initiatives, and determining whether the Department's IT governance model results in effective use of taxpayer resources and promotes sound IT security practices. DOI, however, faces organizational challenges with IT infrastructure, IT security, IT resource management, and

IT governance. Recognizing these ongoing challenges, for FY 2015, OIG requested and received funding for two additional IT audit staff for these IT reviews. We requested, but did not receive, funding for FY 2016 to dedicate staff to an Insider Threat Program. Our proposed FY 2017 budget requests another two IT staff for cyber security audits.

OIG also included IT security as one of the Department's Top Management Challenges in FY 2013 and again in FY 2014. DOI relies on complex, interconnected information systems to carry out its daily operations. Specifically, DOI spends about $1 billion annually on its portfolio of IT assets, which supports programs that protect and manage our Nation's natural resources and cultural heritage; provides scientific and other information to the public about those resources; and meets the Department's responsibilities to American Indians, Alaska Natives, and affiliated Insular Areas.

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to establish an information security program that incorporates eight key components, and each agency inspector general to annually evaluate and report on the information security program and practices of the agency. The U.S. Government Accountability Office (GAO) found that the extent to which agencies have implemented security program components showed mixed progress. New guidance emphasizes continuous monitoring as a key technology in agency attempts to improve cyber security and reduce risk by keeping a constant check on the effectiveness of security controls and the level of current threats. By approaching IT security as an ongoing review area rather than a limited engagement, OIG can provide timely and meaningful solutions to help DOI improve safeguards over the confidentiality, integrity, and availability of information resources.

FISMA requires agencies to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency IT assets. To satisfy annual reporting requirements, agencies expend large amounts of money and resources to document compliance with 11 FISMA reporting areas. An agency's FISMA score (its compliance rate) has been found, however, to be unrelated to whether its IT assets are adequately protected from attack.

More recent FISMA guidance has shifted the focus of agency oversight from periodic assessments and compliance reporting to using tools and techniques to conduct ongoing monitoring of IT security controls. A well-designed and well-managed continuous monitoring program can transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential information about a system's security status on a real-time basis. This, in turn, enables officials to take timely risk mitigation actions and make risk-based decisions regarding the operation of their IT systems.

This is precisely what we did in the IT audit at issue in today's hearing. The results of our efforts provided the bureaus with the real-time information necessary for them to take prompt action. A future OIG follow-up audit will determine whether those actions were effective at addressing the vulnerabilities identified.

Summary of Report

"Defense in depth" is a widely recognized best practice for protecting critical IT assets from loss or disruption by implementing overlapping security controls. The concept of defense in depth is that if one control fails then another is in place to either prevent or limit the adverse effect of an inevitable cyber attack. We found that three DOI bureaus had not implemented effective defense in depth measures to protect key IT assets from Internet-based cyber attacks.

Specifically, we found nearly 3,000 critical and high-risk vulnerabilities in hundreds of publicly accessible computers operated by these three bureaus. If exploited, these vulnerabilities would allow a remote attacker to take control of publicly accessible computers or render them unavailable. More troubling, we found that a remote attacker could then use a compromised computer to attack the Department's internal or nonpublic computer networks. The Department's internal networks host computer systems that support mission-critical operations and contain highly sensitive data. A successful cyber attack against these internal computer networks could severely degrade or even cripple the Department's operations, and could also result in the loss of sensitive data. These deficiencies occurred because the Department did not: (1) effectively monitor its publicly accessible systems to ensure they were free of vulnerabilities, or (2) isolate its publicly accessible systems from its internal computer networks to limit the potential adverse effects of a successful cyber attack.

Moreover, in recognition of increased cyber threats to Government systems, on May 21, 2015, the U.S. Department of Homeland Security (DHS) mandated that Federal agencies mitigate all critical vulnerabilities in publicly accessible systems within 30 days. Using the DHS definition of "critical vulnerability," we provided the results of our vulnerability testing, where we identified 668 critical confirmed vulnerabilities in various bureaus' publicly accessible systems, to the Department in January and February 2015.

The results contained in this report are the first in a series on defense in depth. We make six recommendations designed to mitigate identified vulnerabilities and strengthen security practices for the Department's network architecture and its public-facing edge, lessen the opportunity for a malicious attack, and minimize the impact and potential opportunities to infiltrate nonpublic systems after a successful attack.

Disclosure of Report

I believe that some explanation is warranted as to how OIG transmitted information regarding this work product.

In light of the recent events in which the personal information of millions of Federal Government employees was breached through the Office of Personnel Management (OPM) IT systems, and the associated heightened focus on IT security by Congress, OIG took the unusual step, 2 weeks ago, of briefing key bipartisan congressional staff prior to the issuance of our final report on our findings regarding IT vulnerabilities at DOI. Subsequent to that briefing, we received a request from a Senate Committee Chair for the draft report upon which our briefing was based. Citing exceptions to our usual protocol, we provided the draft report to the Chair and Ranking Member of that Committee, as well as to the other Committees that were represented at the bipartisan briefing, including this one.

As we explained to the recipients of our briefing, we made exceptions to our standard process associated with this report for several reasons: (1) because of the importance of our findings related to IT security; (2) because the affected DOI bureaus have been aware of our findings for some time; and (3) to take advantage of the sense of urgency that has resulted from the OPM breach. For these reasons, we also significantly reduced the amount of time we provided for the Department to respond to our draft report to only 14 days. We received the Department's response on July 9, 2015.

Our normal practice is to issue a draft report to the Department and await its response before disseminating it further. This practice is consistent with Government Auditing Standards as it allows for an exchange with responsible officials to ensure that the report is fair, complete, and objective prior to it being issued in final form. In this instance, shortly after our briefing of

congressional staff, we met with the Department to discuss the draft report, learned that the Department would concur with all our recommendations, and discussed limited areas in the report that will need to be edited for clarity and accuracy. The final report will, therefore, differ slightly from the draft report, although we expect the findings and recommendations to remain at least substantially the same. We intend to remove the identities of the affected bureaus and any other identifying information from the final report in the version that will be made available to the public, to minimize the risk of the information contained in the report being used for improper purposes.

Mr. Chairman, Madam Chairman, this concludes my prepared remarks today. I will be happy to try to answer any questions that you or members of the Subcommittees may have.

Mr. HURD. Thank you, Ms. Kendall.

I would now like to recognize the ranking member of the Interior Subcommittee, Mrs. Lawrence, for 5 minutes for opening remarks.

Mrs. LAWRENCE. Thank you, Mr. Chairman. I want to thank you for holding this hearing and examining the effectiveness of the Department of Interior's cybersecurity practices. I also want to thank our witnesses for speaking with us today. I know some of you are returning.

Recent cyber attacks in public and private sectors highlight the importance of enhancing information security policies and controls. Although the Department of Interior has not suffered a breach of its data in relation to cyber attacks on OPM, information security weaknesses have been identified by the inspector general and exploited by cyber attackers.

The Federal Information Security Management Act, or FISMA, requires each Federal agency, and I will quote, "each Federal agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency," end quote.

In the Office of Management and Budget annual report to Congress on FISMA for fiscal year 2014, the Department was at or above compliance standards for several areas of affected information security. According to OMB's report, the Department was given an overall cybersecurity assessment score of 92 percent, 16 percentage points higher than the average score for reporting agencies, which was 76 percent.

However, I'm concerned that the Department was identified as having weak profile, which means that the majority of unprivileged users are allowed to log onto network systems with a user ID and password alone. This is an increased risk of unauthorized network access.

In closing, today's hearing provides an opportunity to gain an understanding from our witnesses of the challenges the Department faces, to learn what DOI is doing to correct their information security deficiencies, and to find out what Congress can do to help ensure that the Department has the people and the resources it needs to enhance its information security practices.

Mr. Chairman, thank you for holding this hearing, and I yield back my time.

Mr. HURD. Thank you, Mrs. Lawrence.

Now to begin our questioning portion of this afternoon, I'd like to turn it over for 5 minutes to Mrs. Lummis, the chair of the Interior Subcommittee.

Mrs. LUMMIS. Thank you, Mr. Chairman. Thanks again for holding this hearing.

And welcome witnesses. Appreciate your being here.

Our committee recently learned through a report of investigation about a high-level IT staffer at the Department of Interior's Office of Law Enforcement and Security. His name is Faisal Ahmed.

Ms. Kendall, can you please quickly summarize the findings of this report?

Ms. KENDALL. Chairman Lummis, thank you.

We have not analyzed the personal privacy security implications of our report in this regard, and so I will not identify the individual by name. But when the OIG was notified that there was an individual in the Office of Law Enforcement and Security who may have falsified his credentials, we investigated these allegations and determined that in fact there were two transcripts suggesting that he had both an undergraduate and a master's degree which he did not have. The person who was subject of this investigation resigned from the position 3 days after we initiated our investigation.

Mrs. LUMMIS. And at the time was Mr. Faisal Ahmed—I'm at liberty to disclose his name—was Mr. Faisal Ahmed the Assistant Director for the Office of Law Enforcement and Security heading the Technology Division?

Ms. KENDALL. I believe that was his title.

Mrs. LUMMIS. Okay. Please continue.

Ms. KENDALL. We did determine that there were two falsified transcripts on the computer that we seized and that those transcripts had been—the individual had requested that the transcripts be included into his official personnel file. Also understand, and this may or may not be in the report that you received, I have since received some information that they may have been submitted for an SES candidate development program. But I understand that the individual was not an SES member as the report may have suggested.

Mrs. LUMMIS. Now, we have reason to belief that Mr. Faisal Ahmed is currently employed at the Census Bureau. Do you know if this is true?

Ms. KENDALL. We were not able to confirm that before the hearing this afternoon.

Mrs. LUMMIS. Have you ever been contacted or have you ever contacted the Census Bureau or Department of Commerce about Mr. Faisal Ahmed?

Ms. KENDALL. We were contacted by an Office of Personnel Management investigator investigating the background of this individual and provided that investigator with the information that we had available in our files.

Mrs. LUMMIS. Now, it's my understanding from the report on investigation on the Faisal Ahmed case that your office presented this case to the Department of Justice, but they declined to prosecute. Do you know anything about why they declined?

Ms. KENDALL. We rarely get reasons behind declinations for prosecution, and I'm not aware of a reason behind this one.

Mrs. LUMMIS. Did anyone from your office have any discussions with DOJ about this case?

Ms. KENDALL. We typically either forward our report of investigation and oftentimes have some discussion with the prosecutors. I could not tell you specifically if we did in this case.

Mrs. LUMMIS. I'm concerned that there may be an individual who was in a high-level position, comparatively, it's high ranking Senior Executive Services position, he had worked, as I understand, at DOI since late 2007, and that he held a security clearance. And so I'm a little concerned—well, I'm more than a little concerned—that he had access to law enforcement sensitive materials and other secure information, that he had falsified his background, and that

now it appears that he is working for another Federal agency, the U.S. Census Bureau.

So there is additional fallout from the issues that have been raised by the gentleman from Texas, Mr. Hurd, about this hearing.

So as to these collateral matters also, I thank you kindly, Mr. Hurd, for holding this hearing. I yield back.

Mr. HURD. The gentlewoman yields back.

I'd now like to recognize my distinguish colleague from Illinois and ranking member, Ms. Kelly, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chairman.

Ms. Burns, the two data breaches OPM recently reported have been particularly concerning to us because of the national security risk involved. According to testimony you gave at a recent hearing on the OPM data breaches, the OPM personnel records that were compromised in one of those breaches were hosted in the data center maintained by the Department of Interior. Did the cyber attackers who gained access to those records also gain access to the Interior Department data center?

Ms. BURNS. So the adversary had access to our data center. It was exposed. There was no evidence based on the investigation that was led by DHS, US–CERT, and the FBI, there was no evidence that the adversary had compromised any other data aside from the OPM data.

Ms. KELLY. Okay, so the same cyber intruder who breached OPM's personal data, which the Department of Interior hosted on its servers, also breached the defense's of the Interior Department data center?

Ms. BURNS. So this, the intrusion that you're referring to, was a sophisticated breach. And my understanding, based on DHS' assessment, was that the adversary exploited, compromised credentials on OPM's side to move laterally and gain access to the Department of Interior's data center through a trusted connection between the two organizations.

Ms. KELLY. So the cyber intruder, did they gain access it to DOI's data center through OPM or was it the other way around?

Ms. BURNS. The adversary gained access to DOI's infrastructure through OPM, as far as I understand, based on DHS's investigation.

Ms. KELLY. Has there been any investigation to determine whether the Department's records were stolen once the attackers gained access to the data center?

Ms. BURNS. So I believe that that was part of DHS' comprehensive investigation. When we first learned from them of the intrusion, they came on board in April 2015, this year, and they actually were on the ground with other interagency partners at the site of the data center, collecting data and forensics for approximately 3 weeks. They took that data back.

So the investigation was ongoing even as they were there. But they took the data back. And my understanding from the report that they issued to us was that there wasn't evidence of further compromise of DOI's data in that data center.

Ms. KELLY. So there is no evidence that the Department's data was stolen.

Ms. BURNS. Correct, based on what DHS' report said. I would defer to them, though, if you wanted to get into more detail, because they did the detailed analysis, and they're really the ones who are the author and the source of the investigation and the findings. But that is my understanding based on reading the report.

Ms. KELLY. In addition to hosting OPM's personnel records, the Department hosts data from other agencies in its data center. Is that correct? And, if so, which agencies?

Ms. BURNS. Yes. Actually, the Department is a—the data center in question, the biggest customer of the data center is actually Interior. So it's the Interior Business Center, what we call IBC. They're a shared service provider, and they are the majority user of the data center. And we also host some applications for the Office of the Secretary in the data center.

Ms. KELLY. Okay. With the exception of the OPM's records, was data from any of the other agencies, those places you mentioned, compromised when hackers gained entry into the Department's data center?

Ms. BURNS. As I was saying before, based on my understanding of the report from DHS and their forensics, there was no evidence that any other data was exfiltrated from the data center.

Ms. KELLY. From all that has happened and what you've gone through, what do you feel are some of the key lessons that the Department has learned.

Ms. BURNS. So many lessons learned. So, as you can imagine, when I as a CIO for the Department learned of the intrusion, it was horrifying to me. And since that time I've been—my team and I have actually been on a high alert, working probably 7 days a week, long hours, to take our lessons learned and do a mitigation plan around it, a remediation plan that's comprehensive.

So lessons learned include things that we were doing already. So, for example, the whole need for two-factor authentication, that's an important control that's needed. We were already working on it, so it was a performance goal that we had for the agency this year, and we had set those metrics for all of our bureaus and offices to achieve certain targets this year, and we were making slow progress to it.

When the incident happened, it just created a different lens on looking at the need, and I think it made it crystal clear to everybody why it was so critical that we achieve two-factor authentication for, first of all, our privileged users, but then also our unprivileged users.

And that's why we were aggressive about moving to getting all of our privileged users using their PIV cards to authenticate to their system. And as I mentioned in my statement, we achieved that on June 26 as part of the Office of Management and Budget 30-day cyber sprint. So it just accelerated the work we had already started.

In addition to that, I was proud to say that we achieved—actually it was at least 75 percent of unprivileged users today.

So people have been working around the clock in my office, but also in the bureaus and offices, because we shared our lessons learned with our other counterparts in our bureaus and offices, be-

cause we have to all own this problem, and it will take all of us to fix the problem, and everybody has been taking it seriously. So I'm very gratified by that.

Ms. KELLY. Thank you for sharing.

My time is up. I yield back.

Mr. HURD. The gentlewoman yields back.

Now I would like to recognize my fellow Texan and colleague, Mr. Farenthold from Texas, for 5 minutes for questioning.

Mr. FARENTHOLD. Thank you, Mr. Chairman.

We've heard testimony that there have been inspector general reports dating back to 2014. We've been talking about cybersecurity here in this committee since well before last year. It's been a pretty critical issue. There are actually some recommendations in the 2014 start of the—in the audit—yet it looks like it really took this data breach to get you guys moving on it.

Ms. Kendall or Ms. Burns, would you like to take just a second and talk about, as a result of 2014, how much was done and how much didn't get done out of the 2014 recommendations? Ms. Burns, I'll let you——

Ms. BURNS. So I wasn't CIO for the Department for the whole time, but as the report was written I assumed the responsibility of this role. We have been working hard, so for me, when I first became CIO, I made cybersecurity a priority. And part of that was because there were things that were happening even before, right before I became CIO.

Mr. FARENTHOLD. But, I mean, you got a huge breach that came in and millions of Federal employees' personal information got out. I mean, you can talk about making something a priority, but it apparently wasn't or we wouldn't have had a breach. Maybe it is impossible to completely stop a breach.

Can we just get a little bit of background, just so everybody is clear on exactly what happened? The Department of Interior, were you hacked or was it an insider or was it a combination of both?

Ms. BURNS. So from my understanding of DHS' investigation, there was a compromise of an OPM privileged account. So there were credentialed, high level—high—a privileged users credentials were compromised and went from OPM——

Mr. FARENTHOLD. Now, do we know if it was an insider job or somebody just got his information, a brute force attack, or some other way, or did he voluntarily share that with?

Ms. BURNS. I don't have that information, and I would defer to DHS, US–CERT, because——

Mr. FARENTHOLD. So how did you all first find out about the breach?

Mr. BURNS. We first found out about the breach because DHS contacted us in April and sat down with me and my CISO and told me that they saw suspicious activity on our network.

Mr. FARENTHOLD. So how confident are we that they're out and that there are no trojans or malware still somewhere in the system?

Ms. BURNS. So, according to DHS, there is no evidence anymore that there is malicious activity.

Mr. FARENTHOLD. I assume you stepped up the monitoring.

Ms. BURNS. Absolutely. Immediately.

So that said, we don't take anything for granted. We're on high alert, because there is the possibility that another breach could happen. And in our discussions with DHS our remediation plan has to include our ability to quickly detect when something bad is happening so that we can shut it down quickly.

Mr. FARENTHOLD. Now, we have also got a July 2015 report that is saying there are potentially thousands of security risks that are still out there. I mean, is all the software up to date? Do you have the security software on all the computers? You' making people change their passwords? How confident are you that you've at least got the basics down?

Ms. BURNS. So within the Office of the Secretary, directly where the breach happened, some of the things we did is remediation, included things like password reset. If you're referring to the IG's report that referenced the vulnerabilities, as soon as we learned about them, I talked with the bureaus in question immediately about them. And as of before the report was actually issued, which I think is going to be soon, the bureaus corrected all the vulnerabilities that were identified in that report.

And so as a follow-up to that, we would like the—I appreciate what the IG is talking about doing in terms of followon to ensure that they check to make sure the vulnerabilities are clearly corrected permanently.

Vulnerabilities, though, it's a process. So it's not something that's a one-time hit. You have to continually do it. It's a process that you have to manage. You have to continually scan, look at what weaknesses exist, categorize the weaknesses so you know what's critical and high, and deploy your resources to the most critical weaknesses that you have that can have the broadest impact on the organization.

Mr. FARENTHOLD. All right, so we're videotaping this and it's being broadcast on C–SPAN 8, the Ocho, or somewhere. The video is out there. If you could talk to your fellow CIOs at other government agencies and give them some piece of advice so this doesn't happen to them, what would be the top two or three things you would tell them? I'll let you answer that and yield back when you're complete.

Ms. BURNS. Okay. First of all, I think that to get this problem fixed that we have in the whole Federal Government it takes strong leadership and drive, but it also takes everybody to help with this. Because cybersecurity isn't isolated to IT. Cybersecurity is a responsibility of everybody. Nobody can abdicate their responsibilities there or else we put ourselves at risk. So that's one thing.

Another thing that I would say is that the FISMA metrics are right, but they are not the only thing that we need to be doing. They're one lens of what we have to be doing, but there is much more.

And I think we have to act in the real world. So it can't be this paper-based exercise that we go through in checking boxes. We actually have to do things like what the IG did, which is get people to actually—it's kind of the red team, blue team type concept—of getting professionals to actually try to attack us, but in a safe environment, so that we can actually understand what the weaknesses are and put them on a list and do something about them quickly.

That would be my advice to my fellow CIOs.

Mr. FARENTHOLD. Thank you very much. And I'll yield back.

Mr. HURD. Thank you, Mr. Farenthold.

Now I'd like to recognize Mr. Cartwright from Pennsylvania for 5 minutes.

Mr. CARTWRIGHT. Thank you, Chairman Hurd.

And welcome to all of our witnesses to are subcommittee.

Ms. Burns, I'm going to ask you some questions. Now, I want you to understand, when I ask you a question, if you don't know the answer, it's all right to say, "I don't know," because accuracy is the most important thing we're after here.

And I share Mr. Farenthold's sentiment that a record is being made today, and I want you to feel free to go back and look at these questions, and if you have more information, provide the information to the subcommittee subsequent to this hearing. Will you do that.

Ms. BURNS. Yes.

Mr. CARTWRIGHT. Ms. Burns, in your testimony from the June 16 hearing regarding the OPM breach, you indicated that the Department of the Interior houses data for the OPM in the Interior Department's data center. Am I correct in that?

Ms. BURNS. Yes.

Mr. CARTWRIGHT. When did the Interior Department first begin hosting data for OPM?

Ms. BURNS. From my understanding in talking with my staff, OPM started to become—first became a customer of the Department in 2005.

Mr. CARTWRIGHT. Okay. Is this under some kind of agreement?

Ms. BURNS. There is a memorandum of understanding between the two organizations.

Mr. CARTWRIGHT. Would you send us a copy of that, please?

Ms. BURNS. We can, yes.

Mr. CARTWRIGHT. Now under that agreement, what is the Department of the Interior's role in providing cybersecurity for the data that it hosts?

Ms. BURNS. So the Department's role—the Department offers OPM our IT infrastructure, so its hosting services, that's what they're consuming from us as a customer. Our responsibilities in terms of security go around securing the IT infrastructure. So that means we provide the data center, which has facilities base, right, the physical security. It has the power and cooling, hardware, the servers, operating system, potentially even the database, and also support services to help OPM just maintain the actual infrastructure in terms of, like, system administrators, database administrators, that kind of thing.

Mr. CARTWRIGHT. I don't mean to interrupt you, but the question is, under the agreement by which the Department of the Interior hosts OPM on its computers, how is cybersecurity treated under that agreement?

Ms. BURNS. So the Department of the Interior, we provide the infrastructure. We are responsible for security the infrastructure. That includes the network connection between us and OPM.

Mr. CARTWRIGHT. Okay.

Ms. BURNS. And we encrypt our connection between OPM and us.

Mr. CARTWRIGHT. How about money? Does the Department of the Interior receive any revenue from OPM for hosting their records on your data center?

Ms. BURNS. Yes, OPM is a customer and we provide our services as a full cost recovery system.

Mr. CARTWRIGHT. Good. How much do you get?

Ms. BURNS. I have to get back to you on that. I'm not sure.

Mr. CARTWRIGHT. Thank you.

Now, in the June 16 hearing you also testified, quote: "DOI also performs shared services for other agencies," unquote. Is that correct?

Ms. BURNS. Yes.

Mr. CARTWRIGHT. Okay. Can you help us understand why the Department is performing data hosting services for other agencies as well?

Ms. BURNS. Yes. So shared services is a concept of creating more robust centralized points of service around specific activities. IT is one of them, but there are others. And it's because you can gain economies of scale. So it's less expensive and more efficient to a customer to consume the service from a provider like that at a better rate. And also, because we can aggregate capabilities in that area of expertise, in this case IT——

Mr. CARTWRIGHT. So the other agencies could store their own data, but it's a cost savings if it's all in Interior, is that it?

Ms. BURNS. It could be for them. They'd have to look at the business case for that.

Mr. CARTWRIGHT. How many other agencies does the Interior Department do this for?

Ms. BURNS. So the primary customer that Interior—what we have in the data center is really the Interior Business Center, so it's an internal customer.

Mr. CARTWRIGHT. I'm looking for a number. How many agencies does Interior do this for?

Ms. BURNS. Can I get back to you on that?

Mr. CARTWRIGHT. Please, please.

Mr. CARTWRIGHT. How long has the Department been hosting data for other agencies?

Ms. BURNS. I don't know the answer to that question.

Mr. CARTWRIGHT. Okay. You'll get back to us?

Ms. BURNS. Yes.

Mr. CARTWRIGHT. Okay.

Now, does the Department provide this hosting function under a similar arrangement, similar to the agreement with OPM?

Ms. BURNS. Yes.

Mr. CARTWRIGHT. So you'll have separate agreements for each of the other agencies?

Ms. BURNS. Yes.

Mr. CARTWRIGHT. Can you get us copies of those as well, please?

Ms. BURNS. We can follow up on that, yes.

Mr. CARTWRIGHT. Thank you.

And I yield back, Mr. Chairman.

Mr. HURD. Thank you. The gentleman yields back.

Now I'd like to recognize Mr. Russell from Oklahoma for 5 minutes.

Mr. RUSSELL. Thank you, Mr. Chairman.

Ms. Burns, the IG found that a remote hacker could exploit vulnerabilities in public accessible computers to attack internal or nonpublic Department of Interior computer networks. Why weren't the two systems not segmented from each other?

Ms. BURNS. So several years ago—actually, if you would indulge me, I need to go back a little bit in history for the Department of the Interior.

In 2001 there was, if you're familiar with the Cobell lawsuit, the Cobell litigation. It was a situation regarding Indian trusts. And as a result of it, there was a breach that caused a decision to disconnect several—it started with disconnecting the Department from the Internet, and it ultimately resulted in about, like, five other bureaus and offices within DOI from being disconnected from the Internet for about 6–1/2 years.

And in this environment, because of just the fear of being disconnected, all the bureaus and offices in the Department basically created sort of the modes and protections around themselves organizationally from an IT perspective. And in essence, you couldn't really work together easily in that environment because they were trying to protect themselves from being associated with trust data.

In 2008, the Department reconnected those organizations back to the Internet, and what it came to find was that the organizations within the Department of Interior had difficulty just doing basic day-to-day work together because of these security controls that were put all around their IT infrastructure. And that initiated an effort to optimize our network. And actually this was not during my tenure, so I'm speaking in the past.

Mr. RUSSELL. And if I can, on that, so we optimized it, but we also optimized it for hackers.

And I guess, Mr. Mazer, you were the CIO for 4 years before Ms. Burns took over. So what efforts, if any, did you undertake to address these issues when you were in charge?

Mr. MAZER. Thank you for the opportunity to respond.

Mr. RUSSELL. Can you move the microphone closer to you?

Mr. MAZER. As Ms. Burns noted, the bureaus are very segmented, they are very fractionated. Before my arrival we embarked upon an effort to say it would be great to have one Department of Interior network providing telecommunications services on behalf of everyone. That started about 10 years ago. There's still ongoing activities that are underway.

But something that emerged out of that was protection on what we call the perimeters. And the perimeters on the network were for—it was the bureaus are making the determination that they would provide protection on the perimeters. At the TICs, the Trusted Internet Connections, is the Department provides protection on incoming and outcoming traffic, but one of the results of the report showed that it is—if people set up Web site servers inside our environment they are liable for exploitation into Interior network operations.

And so, I always counseled, whenever we had an incident—and we had an incidents, whether its malware or APT, advanced per-

sistent threats—was when our team became aware of it we would work with that Bureau and all that to remove the particular affected server from there.

I also encourage people that were hosting Web sites: Please, for gosh sakes, get off of the environment, put yourself into a separate enclave. So one of the efforts that occurred during my tenure is the Department embarked upon a cloud solution for public Web sites. So the DOI.gov quite a few of the Web sites that we are seeing, they are all migrating to a public—a government cloud service provider that has a FedRAMP moderate categorization on those activities.

Mr. RUSSELL. And I guess we see—Intel 101 says compartmentalization is good, because it creates barriers. It also creates efficiency problems, we acknowledge that. So my question for Ms. Kendall or Mr. Gilkeson, as I yield back my time at the conclusion, is how do we balance the optimization with the security and what would you recommend for the fix?

Ms. KENDALL. I think Mr. Mazer identified the cloud as being one of the fixes. We had several recommendations, six, I believe, total in this report, but the cloud was one of them. The other was to remove these outward-facing computer systems from being connected to the inside of Interior's systems so you could provide information to the public, to the outside without access or connectivity and compromise to the internal.

Mr. RUSSELL. Thank you. I yield back my time, Mr. Chairman.

Mr. HURD. Thank you, sir.

I'd now like to recognize Ms. Lawrence from Michigan for 5 minutes.

Mrs. LAWRENCE. Thank you, Mr. Chair.

Ms. Burns, what is the Department's plan and time line for implementing the IG's recommendations?

Ms. BURNS. So we're doing some things immediately. I have already—as soon as I saw the draft report and what findings and recommendations were, I started to talk with all of our bureau IT leaders about things that we needed to do. So we are engaged in conversations with our bureaus and offices right now about things that we want them to do right away to mitigate the situation that was identified in the IG's report.

That's a short-term action, because of the real issues, right, and the threats, the vulnerability, the weakness it presents to the Department. There is longer-term things that we need to do, and some of those longer-term things go to things like network segmentation.

A form of network segmentation, as in the previous question, is creating what they call DMZs, what they call an—it's a demilitarized zone, it's basically a safe place, right, to put externally facing systems and configure them in a certain way where they are secure and they don't do what was described in the IG's report.

So some of the immediate actions that we have, we can tell everybody, give them guidance on what they need to do right now. Longer term, I believe we need to move to a consolidated enterprise-wide DMZ for publicly facing systems, and as the IG's office was also saying, embracing the cloud more for our systems.

Mrs. LAWRENCE. Do you, sitting here today before this body in this hearing, do you see any obstacles that would stop you from addressing these concerns or would cause you a challenge that we need to know about?

Ms. BURNS. Right now I think we're—I feel very fortunate in that we have the full cooperation of the organization at every level. If there's one big impediment, it would be that, it would be resistance, I'm happy to say right now, and I think it's because of just the stark reality of the threats and it hit home for DOI, that everybody is cooperating and doing the right thing and they want to do the right thing. So leading that effort I think will be easier because we have the full cooperation at all levels.

Mrs. LAWRENCE. The first recommendation for the CIO is to require and enforce the secure development and management of all publicly available IT systems.

Mr. Burns, what are you doing to require and enforce information security improvements across the various bureaus of the Department? I'm sorry, Mrs. Burns.

Ms. BURNS. Thank you. Thank you.

So actually I have to thank you all for passing FITARA, because I think FITARA is pivotal legislation that helps us to drive the consolidation and centralization of the things that we're talking about today.

I think some of the—one of the biggest challenges that the Department has is the fact that you have all the different separate operating environments for IT. That has to come under kind of a single presence of mind, if you will, under the CIO.

And so there are challenges in the bureaus and offices even with programs who are in far-flung places in the country who are doing whatever they're doing because it's the best way they know to do their job, but they're not getting any direction, central direction from their bureau and from the Department.

I think that FITARA positions us to fix that problem, and the Department is very committed to following through and taking advantage of all the provisions of FITARA.

Mrs. LAWRENCE. Mr. Mazer, you're the former Interior CIO. Do you agree that there are challenges to dealing with multiple bureaus? And do you feel that we are on target to meeting the requirement to enforce security improvements?

Mr. MAZER. I used to work in intelligence, so it's always trust, but verify within the IG. We looked at, when we did this one particular job or activity on the Web inspection, that was just one area of vulnerability in the broad surface of what could confront the Department.

Web sites are very easy to do hacks on, they are very easy to do activities on. We do want to do examinations on how well the credentials, are people using two-factor authentication, are they having too many—are there too many elevated privileges for users on applications.

We're looking at activities like we're all in a mobile world, what does everyone have when they're taking things away with them? We're looking at assuring that there is mobile device management put in place on any particular devices that our people are looking at.

We are also looking at interconnection agreements in terms of what will we have with different agencies if we are acting as a shared services type of providers. And in some of those interconnection agreements and all, if they have those, we want to assure that they are coming underneath a Trusted Internet Connection, those TICs that provide that perimeter protection from the outside world.

Some of the agencies might be doing direct circuits, they might be encrypted, they might not be. Some agencies are using a thing that is called MTIPS, which is outside of an agency's way of monitoring Internet traffic.

So it remains to be seen. We are very gratified and pleased by the progress of the Department in responding to the Web inspection activity. When the Department in the past would do these things, during Ms. Burns' tenure or mine, the ability to do scans on those network perimeters was very limited. We might only use just one particular scanning tool or another scanning tool that might come up with a couple of hundred vulnerabilities. If you had an organized advanced persistent adversary that used a variety of tools, it really illuminated to the Department and all that the steps that need to be taken.

Mrs. LAWRENCE. Thank you.

I yield back.

Mr. HURD. Mr. Blum, you're recognized for 5 minutes.

Mr. BLUM. Thank you, Chairman Hurd.

And I'd like to thank the panel for being here today and giving us your insights on these most critical issues.

Ms. Burns, I believe 20 of the 29 IG recommendations made in fiscal year 2013 in the audit remains open. Many of these are basic cybersecurity recommendations, as you're well aware, such as implementing third-party vendor security patches, maintaining an up-to-date information systems inventory, and utilizing approved and authorized solutions for remote access.

When do you expect to address these recommendations?

Ms. BURNS. So those are on a rolling list that my team keeps and we monitor very closely with specific targets. I'd have to go back and look specifically to see what our plans are, what we had as the date for doing that.

Ms. BURNS. But I would say that with all the events of the past few months there's heightened attention to all things related to cybersecurity. We were already working on, for instance, clauses to contracts that would include security provisions. And so those things were already underway.

Mr. BLUM. Do you plan on implementing all of them?

Ms. BURNS. We would like to implement the things that—I think if we agree with them, we want to implement them.

Mr. BLUM. Did many of these stem from before your tenure as CIO?

Ms. BURNS. Yes, sir.

Mr. BLUM. So that would be Mr. Mazer then, is that correct?

Mr. MAZER. That would be correct.

Mr. BLUM. What did you do, Mr. Mazer, in your tenure to address these? Twenty of the 29 remain open today. What did you do to address these during your tenure?

Mr. MAZER. What we would do with, regardless of any weaknesses or we'd call them program objectives and milestones, is we literally receive thousands of weaknesses.

What I did during my time, and it appears that it is continuing, is we set up a particular organization, sub-organization within the OCIO that monitored all audit and GAO and weakness findings. And then we pressed upon the bureaus or the office that was responsible for them on completion dates. And then there was a continuous follow-up on whether or not they are finishing those recommendations to be completed.

Some recommendations can't be finished within 2 months, 4 months. Some might take a particular year because it might have to take a clause and a contract change.

Mr. BLUM. Twenty of 29 seems to be a big number to me, and they're still open today.

Mr. MAZER. If you look at open findings or open audit actions in all that, there is literally—there might be several hundred of those. There are normal things that are either a weakness in all that, that need to be corrected, and then they will be corrected. The bureaus have always been or the office who is responsible for that are always pressed to get updates, they are requested for updates as to when those things are going to be done.

Mr. BLUM. The IG felt these were important enough to put them on a list. And it seems like the list, it never makes it to the top of the list. And it sounds like it hasn't for years. That concerns me. Does it concern you, Mr. Mazer?

Mr. MAZER. It very much concerns me. When we looked at things like—we call the term POAMs, forgive the abbreviation—there are literally thousands of them. One of the things that we were looking at and it is still continuing under Mrs. Burn's tenure is how many of these things are older than 6 months and then what were the steps in all that, that needed to be to complete those.

Mr. BLUM. Were you eligible to receive a bonus over the last 3 years as CIO?

Mr. MAZER. Yes, sir.

Mr. BLUM. Did you receive a bonus in 2011?

Mr. MAZER. Yes, I did.

Mr. BLUM. Did you receive a bonus in 2012?

Mr. MAZER. Yes, I did.

Mr. BLUM. Did you receive a bonus in 2013?

Mr. MAZER. Yes.

Mr. BLUM. Ms. Burns, did you receive a bonus in 2014?

Ms. BURNS. Yes.

Mr. BLUM. I have a minute left. My last question, Ms. Burns, if there were another hack of the agency's servers in the Department of Interior today, what could the hackers do? What kind of damage could be done? Could they access other areas of the Department of Interior servers? Could they access other agencies' information if it happened today?

Ms. BURNS. There are risks to the Department. And so it is important for us, for me to be attentive to what's going on and make sure that we do whatever is necessary to immediately—and I'm not talking about waiting years, I'm talking about looking at what could really happen to us and damage us and act quickly. And

that's something that I have been doing. I was doing it during my tenure. But I think it is with sharpened focus since over the past few months.

Mr. BLUM. Are we still vulnerable? Is that a yes? Are we still vulnerable? Can they still do serious damage today?

Ms. BURNS. I think that all agencies are vulnerable.

Mr. BLUM. Thank you are for your candor.

And with that, I yield back my time, Mr. Chairman.

Mr. HURD. Thank you, Mr. Blum.

Votes are going to be called soon, and I think we can get through the questioning before then. I would like to turn it over to Mr. Lieu for 5 minutes.

Mr. LIEU. Thank you, Chairman Hurd.

Ms. Burns, at the Department of Interior's data center, you don't house the CIA's list of covert spies at that data center, correct?

Ms. BURNS. Correct.

Mr. LIEU. And you don't house our Nation's classified nuclear launch codes at that data center, correct?

Ms. BURNS. Correct.

Mr. LIEU. In fact, you didn't house OPM's security clearance database either at that data center, right?

Ms. BURNS. Correct.

Mr. LIEU. And that's because you're not a national security or intelligence agency, correct?

Ms. BURNS. That's correct.

Mr. LIEU. So I am going to read you the mission statement of your Department, which is: "The Department of the Interior protects and manages the Nations natural resources and cultural heritage; provides scientific and other information about those resources; and honors its trust responsibilities or special commitments to American Indians, Alaska Natives, and affiliated island communities."

And with the indulgence of the chair, I would like to put this into the record.

Mr. HURD. So moved.

Mr. LIEU. Mr. Chair, I would also like to enter into the record the mission statement of OPM, which is the following: "Through our initiatives, programs, and materials, we seek to recruit and hire the best talent; to train and motivate employees to achieve their greatest potential; and to constantly promote an inclusive workforce defined by diverse perspectives. OPM provides human resources, leadership, and support to Federal agencies and helps the Federal workforce achieve their aspirations as they serve the American people."

Mr. LIEU. OPM is not a national security or intelligence agency either, isn't that correct?

Ms. BURNS. It doesn't seem so.

Mr. LIEU. Right. So I just want to make a point that for the same reasons we don't house our crown jewels of American intelligence at Department of Interior, there is no way we should be housing it in a human resources agency.

Now, I would like to move on to the actual database that was breached at your data center, which was the 4.2 million personnel records that were not the security clearance records. OPM testified

in one of the earlier hearings that they didn't encrypt their information because it was in COBOL language and they said they couldn't do that. But that's not true, right? COBOL can, in fact, be encrypted. There is nothing that says you cannot encrypt something written in COBOL, isn't that correct?

Ms. BURNS. I am not an expert in COBOL, so I can't answer that question.

Mr. LIEU. If you could get information back to us on that, that would be terrific.

Ms. BURNS. Yes.

Mr. LIEU. And then let me ask you, when they breached the systems through OPM into your data center, you said that no other information was compromised. Is that because the hackers found other information uninteresting? In other words, they could have gone to all these other databases and they chose not to? Or did you actually have protections there that prevented them from going to other databases that you were housing and storing?

Ms. BURNS. So I can't speculate about the motives of the attacker. What I know from the assessment that DHS performed, and they are the best source to talk about the specifics of the forensics that happened, there was no evidence of compromise of other data aside from OPM.

Mr. LIEU. Let me ask this another way. If someone is in your data center in one database, can they look at your other databases of other agencies or of your own Secretary's information?

Ms. BURNS. So I would want to confirm this with my team, but I believe the answer to that is no. We use access controls and other methods to protect the data, other data in the data center that is different, aside from the OPM data.

Mr. LIEU. Is that no now or no at the time or both?

Ms. BURNS. I'm sorry, could you repeat it? I didn't hear.

Mr. LIEU. If it's no, was that also the case when this breached happened?

Ms. BURNS. Yes.

Mr. LIEU. Or was it fixed later?

Ms. BURNS. No. It was always that way.

Mr. LIEU. Okay. Thank you.

And then let me conclude by commending you. You said something that I found important. You said: We own this problem. So I appreciate that you said that. It shows that you understand that it is not the responsibility of foreign enemies or hackers to protect our systems, it is our responsibility; that you understand the gravity of this issue; and that your view is we are going to try to prevent breaches, and that you are not going to measure your success by happening to find a breach 4 months later or a year later, that you are going to try to prevent these breaches in the first place.

So I appreciate that and look forward to working with you.

Ms. BURNS. Thank you, sir.

Mr. LIEU. I yield back.

Mr. HURD. The gentleman yields back.

Mr. Palmer from Alabama for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman. And I would like to thank the witnesses for coming.

Ms. Burns, I think it's been established that there were known vulnerabilities and that the Department of Interior had suffered actual attacks that exploited some of these vulnerabilities prior to your team coming in, is that correct?

Ms. BURNS. I'm sorry, I can't hear you. Can you repeat the question? Sorry.

Mr. PALMER. Okay. What I was saying is, is that there were known vulnerabilities and that the Department of Interior had suffered actual attacks that exploited these vulnerabilities prior to your coming on, is that correct?

Ms. BURNS. I believe that is correct.

Mr. PALMER. So you knew that there were vulnerabilities. And you are also aware, I would assume, that the Sakula malware, which has been tied to the OPM attack, had been also tied to the Anthem cyber attack. Were you aware of that?

Ms. BURNS. I participated in briefings with DHS and OPM.

Mr. PALMER. Did it not occur to you that you needed to evaluate the vulnerabilities at DOI for a potential cyber attack from what we knew in terms of the malware that was used in the Anthem attack?

Ms. BURNS. So I think I need to clarify that from my understanding of the incident that involved OPM——

Mr. PALMER. I'm talking about going back. You knew there were vulnerabilities, you knew that there had been prior attacks. We also knew that the Sakula malware had been used in the Anthem attack. Did no one, did it not occur to anyone that such an attack on the scale of the Anthem attack might could occur at DOI?

Ms. BURNS. So I think that we have to be, as I said, on alert about the dangers that are out there in terms of cybersecurity.

Mr. PALMER. No, ma'am. That's a yes or a no. You either did the due diligence or you didn't.

Ms. BURNS. Could I, if I could, with greatest respect, just clarify that the breach from OPM into DOI did not happen because of a vulnerability in DOI's data center. It happened because of compromised credentials of a privileged user on OPM's side that then moved into DOI's environment. So it was not because of a vulnerability.

Mr. PALMER. Well, all right. Thanks for making that clarification.

Mr. Mazer, you were the Chief Information Officer for 4 years before Ms. Burns took over. What efforts, if any, did you undertake to address these issues when you were in charge?

Mr. MAZER. When I assumed the role of the CIO at the Department of the Interior, the Department of Interior was basically predicated, the CIO's office was a policy shop. The CIO's office would promulgate policy to the respective bureaus and offices to assure that they were taking care of things like security, capital planning, enterprise architecture, systems life cycle development.

I embarked upon—for 6 months we worked on a draft, it became known as the 3309 Secretarial Order, which says we need to consolidate Clinger-Cohen functions, like capital planning, enterprise architecture, and security underneath one CIO. And then we also stated that we need to move common infrastructure that everyone uses underneath one particular entity. We worked on a strategic

plan. Arising out of the strategic plan, we settled on things that we called service towers.

Mr. PALMER. I've only got a minute left.

Mr. MAZER. Yes, sir. I'm sorry.

Mr. PALMER. I appreciate the detail of the answer. And if you'd like to put the balance of that in writing and provide it to the committee, you're welcome to do so.

Mr. MAZER. I'd be more than delighted. Okay.

Mr. PALMER. I'd also like to know, was the database that the Interior hosted, including the OPM, encrypted?

Ms. Burns.

Ms. BURNS. I'm probably not the right person to ask about that because OPM is the owner of the data. And I, in sitting in the testimony with the previous OPM Director, I just heard her testimony that she said the data was not encrypted. So I get my information from that. I would have to check with my technical team.

Mr. PALMER. Do you have any idea how many serious breaches DOI has suffered in 2014?

Ms. BURNS. I'm sorry, could you repeat that?

Mr. PALMER. So far for this year, how many breaches have you suffered? Do you have any idea?

Ms. BURNS. In 2015?

Mr. PALMER. In 2014–2015.

Ms. BURNS. So that—I can't answer that. We have a distributed IT environment, as I said, and there is a—it was cited in the IG's report that there was a—reports of incidents, I think they referred to some incidents in the report, that were reported by the bureaus and offices that my office doesn't necessarily have visibility into. So we have to do research into them. In order to answer your question, I would have to go back and look further at that.

Mr. PALMER. Would you be willing to let the committee know that?

Ms. BURNS. Yes.

Mr. PALMER. Thank you.

I yield, Mr. Chairman.

Mr. HURD. Thank you, sir.

I'd like to yield myself 5 minutes.

I just want to be clear, Ms. Burns, because you make a good point and I want to make sure everyone recognizes that. The bad guys got access to a credential that was OPM and they used that credential to gain access to the data housed at the Department of Interior. So that they used those credentials that had natural access to the information that was breached, is that correct?

Ms. BURNS. That's correct.

Mr. HURD. So they didn't take advantage of any vulnerability other than getting access to that user name and password.

Ms. BURNS. That's my understanding, sir.

Mr. HURD. Thank you.

This recent vulnerability assessment that the inspector general did, who called for that?

Ms. KENDALL. We initiated it ourselves, sir.

Mr. HURD. Okay.

And, Ms. Burns, how much of the IT budget for Department of Interior do you control? First question, what's the IT budget roughly for all of DOI?

Ms. BURNS. So the IT budget overall, we report approximately a billion dollars a year.

Mr. HURD. So of that billion dollars, how much do you, as the CIO of the Department, have access to?

Ms. BURNS. I would say it's——

Mr. HURD. Roughly.

Ms. BURNS. It's approximately less than $200 million.

Mr. HURD. So you are the CIO of the entire Department and you have access to less than $200 million. Isn't that a problem?

Ms. BURNS. I think that the provisions that you gave us in terms of authorities to CIOs in FITARA, whereby I have to approve IT spending, helps. Even though I don't have the money, all the funds for the IT portfolio in my direct budget, it gives me significant influence.

Mr. HURD. You have a little bit more control, is what you are saying.

Ms. BURNS. Yes.

Mr. HURD. Now, let's focus on the assessment that was done. The draft report that we have access to said that nearly 3,000 critical and high-risk vulnerabilities in publicly accessible computers operated by three DOI bureaus was found, is that correct?

Ms. BURNS. Yes.

Mr. HURD. Have all those been remediated?

Ms. BURNS. From my understanding, yes.

Mr. HURD. But I also have information that indicates—and, Ms. Kendall, you may be able to confirm this—that the Department of Interior's total number of publicly accessible computer is unknown because the Department doesn't perform discovery scans of their publicly accessible information, is that correct?

Ms. KENDALL. I believe that's correct based on what we conducted in terms of——

Mr. HURD. So that number could be significantly higher than 3,000?

Ms. KENDALL. It could be.

Mr. HURD. And there could be——

Ms. KENDALL. No, I'm sorry, I believe the 3,000—and I'll ask this—was the vulnerabilities.

Mr. HURD. The total vulnerabilities?

Ms. KENDALL. Yes.

Mr. HURD. Okay. So the number of publicly accessible Web sites that have these vulnerabilities is higher than what it is because we don't know the total summation of those?

Ms. KENDALL. It could potentially be, yes.

Mr. HURD. So I would have liked—and, again, if this is publicly accessible information, those three bureaus that's doing it, that is not classified information because the bad guys can figure that out. That's just a point for me. Because I would have liked those three CIOs to be here, because they probably have a budget probably larger or in line with yours, is that correct, Ms. Burns?

Ms. BURNS. I can't tell you. I don't have that information with me right now.

Mr. HURD. So the remediation of those three bureaus, was that overseen by your office or was that overseen by CIOs from these varies bureaus?

Ms. BURNS. The remediations ultimately would have been overseen by—so we don't call them CIOs, we changed that when that secretarial order was issued. We call them Assistant Directors for Information Resources. And they—so they head IT in the bureaus. But I would tell you that IT in the bureaus is not centralized under them. So while they would oversee the mitigation of the vulnerabilities that you're talking about, those vulnerabilities could have resided at a lower program level that was outside of the chain of command of the bureau.

Mr. HURD. Mr. Gilkeson, maybe you're the right one. Isn't that pretty outrageous for designing management control of an IT system?

Mr. GILKESON. It's certainly not optimal, Mr. Chairman, I would say.

Mr. HURD. I'll take that.

Mr. GILKESON. It's a very—it's a highly decentralized organization. I think that's kind of coming through.

Mr. HURD. Is there a move afoot, Ms. Burns, to centralize some of this information?

Ms. BURNS. Yes, there is, sir. Under FITARA and our implementation plan for FITARA, there are plans to bring that more under a centralized management.

Mr. HURD. And I would like, without objection, to submit the Department of Interior's response to the IG report to the record.

Mr. HURD. And in this report, they talk about—you all talk about how long it's going to take to fix all the problems that the IG report identified. When do you think all those are going to be done?

Ms. BURNS. Some of it is dependent on resources because I have limited staff to be able to do stuff. I think that at the same time it's my obligation to be prudent about how we use the money that we have, and that includes leveraging the bureaus and offices as much as possible to be able to fulfill the fixes that go along with the recommendations.

So, as I said, we do the best we can with the resources that we get. There are some immediate things that we can do to protect us against the immediate threat. And, as I mentioned, I'm already talking with the bureaus and offices about those things so we can take immediate action.

Mr. HURD. Great.

Ms. BURNS. The longer term things do have cost.

Mr. HURD. And, Ms. Burns, I want to join my colleague from California in thanking you for taking responsibility for this. And you said something else in your opening remarks that I am going to have to go back to the record and write down: This not just a paper-based exercise, you've got to roll up your sleeves and actually do something. And I appreciate that mentality. But I also want to make sure that—what were the people that you called, they're not CIOs of bureaus anymore, Assistant——

Ms. BURNS. We call them ADIRs.

Mr. HURD. Let your ADIRs know that they should be sitting alongside you as well. And I appreciate you being here to answer

the questions for the folks that are all in the organization of DOI who have the responsibility for fixing some of these issues. And I recognize it is not necessarily all in your area of control as it should be.

And so we want to make sure that we continue looking at things like FITARA and FISMA and how we can strengthen your control over these issues, because we are going to be holding you responsible. And if we are going to hold you responsible, you should have the tools to fix the network.

So I want to appreciate everyone for coming out today. This is an important topic. I'd like to yield a minute to my colleague from Texas.

Mr. FARENTHOLD. Thank you. I realize we are in a hurry for votes. I was next door dealing with the excessive regulation in the EPA. But Jeff from my office says both Ms. Burns and Ms. Kendall spoke positively about moving more information and more of the IT to the cloud.

And I just wanted to get both of you all to quickly tell me if there is anything that Congress can do to help enable that and move that along.

Ms. BURNS. From my perspective, I am appreciative for what you did with enacting FITARA and the new version of FISMA. I think they help us greatly. And before I would ask you to do anything more, I would say let us take the tools that you have given us and try to do the best we can to make them work in our organizations.

Mr. FARENTHOLD. Ms. Kendall, do you want to add anything?

Ms. KENDALL. I would only add that when we briefed staff on this report, one of the questions was what kind of financial resources need to come along to make these things happen. And the IG does not make those recommendations. But I would encourage the Department to provide that information to you as well because I think it is very much resource driven.

Mr. FARENTHOLD. Thank you all for being here. And thank you for your work.

Mr. HURD. Without objection, I would like to provide the—put the IG report on Faisal Ahmed on the record. And without objection, so ordered.

Mr. HURD. And I'd like thank our witnesses for taking the time today and appearing before us. This is an important issue and something that this subcommittee is going to continue to investigate.

And, Ms. Burns, you know, this is—we are here to be supportive and make sure that you have all the tools you'll need to do your job.

Thank you all. And the subcommittees stand adjourned.

[Whereupon, at 4:01 p.m., the subcommittees were adjourned.]

APPENDIX

Material Submitted for the Hearing Record

U.S. OFFICE OF PERSONNEL MANAGEMENT

OUR MISSION, ROLE & HISTORY WHAT WE DO

Through our initiatives, programs, and materials, we seek to recruit and hire the best talent; to train and motivate employees to achieve their greatest potential; and to constantly promote an inclusive work force defined by diverse perspectives.

OPM provides human resources, leadership, and support to Federal agencies and helps the Federal workforce achieve their aspirations as they serve the American people. " We're responsible for keeping the government running smoothly — a responsibility that has daily consequences for every citizen.

We've set our sights on making the U.S. Federal Service America's model employer for the 21st century, with the following clear and measurable objectives:

- Make searching and applying for Federal jobs easier and faster;
- Provide Federal employees benefits that are relevant, flexible, fair, and rewarding;
- Make Federal employment accessible — and possible — for every American who seeks it; and
- Retain a Federal workforce as diverse and versatile as the work it does and the people it serves.

The men and women of the Federal Service are ready to attend to America's needs for safety, security, and prosperity. We're here to keep them energized, equipped, and fully engaged.

Policy and Oversight

OPM oversees all policy created to support Federal human resources departments — from classification and qualifications systems to hiring authorities and from performance management to pay, leave, and benefits. Along with making those policies, we are responsible for ensuring they are properly implemented and continue to be correctly carried out.

Healthcare and Insurance (HI)

Healthcare & Insurance ensures the availability of quality benefits for the Federal family. We work to facilitate access to the high-caliber healthcare and insurance programs offered by the Federal Government, including: health services; dental and vision benefits; flexible spending accounts; life insurance; and long-term care programs. HI also develops and administers programs that provide high quality and affordable health insurance to uninsured Americans through Affordable Insurance Exchanges, uninsured Americans with pre-existing medical conditions who cannot otherwise purchase coverage, and employees of tribes or tribal organizations. .

Retirement Services (RS)

Subscribe

Email Updates
Sign up to stay informed about the latest happenings at Interior.
Enter your email address for updates Submit

Mission Statement

Protecting America's Great Outdoors and Powering Our Future

The Department of the Interior protects and manages the Nation's natural resources and cultural heritage; provides scientific and other information about those resources; and honors its trust responsibilities or special commitments to American Indians, Alaska Natives, and affiliated island communities.

-- from the DOI Strategic Plan

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

JUL 9 2015

To: Kimberly Elmore
Assistant Inspector General for Audits, Inspections, and Evaluations

From: Sylvia Burns
Chief Information Officer

Subject: Office of Inspector General, Draft Evaluation Report, Security of the U.S. Department of the Interior's Publicly Accessible Information Technology Systems, Report No. ISD-IN-MOA-0004-2014

The Department of the Interior (Department), Office of the Chief Information Officer (OCIO), appreciates the opportunity to review the Office of Inspector General (OIG) draft Evaluation Report (Report), Security of the U.S. Department of the Interior's Publicly Accessible Information Technology (IT) Systems, ISD-IN-MOA-0004-2014. Attachment 1 provides the Department's Corrections and Comments to the draft Report. Attachments 2 and 3 provide the Department's Summary Response and the OCIO Statement of Actions to implement the OIG's draft recommendations. They serve as a preview of our formal response given the contents of the draft Report. The Department will update these attachments as appropriate based on the OIG's final Report.

The Department supports and appreciates the OIG's work in assessing and advising on the potential vulnerability of its information technology systems to outside intrusions. This vulnerability assessment provides valuable information about potential vulnerabilities that assists greatly in the Department's ongoing efforts to strengthen data security. Accordingly, the Department and its bureaus fully cooperated with the OIG upon being advised of this assessment. The Department accepts the OIG's recommendations, and will incorporate them into a Departmental cyber security action plan. Further, the Department is engaging all bureaus and offices in discussions about the OIG's findings and the need to undertake major changes in how we manage publicly facing systems across the entire Department. The impacted bureaus report that the vulnerabilities identified in the Report have been corrected or are in the process of being addressed. The OCIO will monitor the correction of any remaining vulnerabilities and require the impacted bureaus to resolve them within the next 30 days.

OCIO recently established a Department-wide cyber security advisory group with experts from a variety of IT management disciplines. The group will advise and support the CIO in developing and implementing a comprehensive, multi-pronged, cyber security strategy and action plan for the agency. The plan will include short, medium and long-term initiatives to strengthen the Department's IT security posture. In addition, the Department's ongoing implementation of Secretarial Order 3309, Information Technology Management Functions and Establishment of Funding Authorities, and the Federal Information Technology Acquisition Reform Act

(FITARA), will address many of the longstanding challenges in IT management identified by the OIG.

The Department appreciates the OIG's evaluation of the security of the Department's publicly accessible computers and its objective perspective on our IT security posture in the interest of promoting excellence, integrity, and accountability in our IT program, operations, and management.

If you have any questions, please contact me at (202) 208-6194 or sylvia_burns@ios.doi.gov. Staff may contact Steven B. Thompson, Acting Director, Internal Control, Audit, and Compliance Management at (202) 821-8887, or steven_thompson@ios.doi.gov.

Attachments:

1. Corrections and Comments to the Office of Inspector General's Draft Evaluation Report
2. Department's Summary Response
3. OCIO Statement of Actions to Address Office of Inspector General Draft Evaluation Report U.S. Department of the Interior's Adoption of Cloud Computing Technologies Report No. ISD-IN-M-OA-0004-2014

Attachment 1

Corrections and Comments to the Office of Inspector General's Draft Evaluation Report

1. Page 3: Reference to exploitations of vulnerabilities in at least 26 incidents. Upon request, the OIG shared the list of 26 incidents referenced in this statement with the OCIO. These incidents are dated from 2012 through 2014. After additional investigation, the OCIO's Incident Response Team confirmed that three of the 26 incidents were false positives.

2. Page 5: Reference to the last sentence under Findings, "The conditions [of inadequate understanding/testing of systems and missing controls for publicly facing systems] can hide significant gaps within the Department's security posture, which questions the validity of any decisions made to authorize the operation of Department and Bureau information systems due to deficient risk awareness." The Department recognizes that the OIG's vulnerability assessment identified weaknesses in the IT security of our publicly facing websites and systems. However, the Department has made significant progress over the past several years in improving our cyber security posture. We have driven Department-wide IT solutions to reduce duplicative investments and systems that unnecessarily increase our IT footprint and threat surface. This includes our financial management system, FBMS, which we recently successfully moved to the cloud, as well as our email system, BisonConnect, which leverages Google Apps for Government in the cloud. We have fully participated in the Department of Homeland Security's (DHS) continuous diagnostics and mitigation (CDM) program and now have nearly full visibility into IT hardware and software assets across the agency along with the ability to centrally patch vulnerabilities. Furthermore, we have strengthened risk awareness throughout the Department at all levels of the organization.

3. Page 14: Reference to "... the recent U.S. Office of Personnel Management and Department's Interior Business Center incidents..." is incorrect. There was one incident between OPM and DOI, so this should say incident rather than incidents. Also, the Interior Business Center's (IBC) Information Technology Directorate (ITD) and the responsibility for the Data Centers were transferred to the DOI OCIO in October 2013. Therefore, the reference to IBC should be removed.

Attachment 2

DOI's Summary Response

Protecting the Department's most valuable data and information is a high priority for the Secretary, the Deputy Secretary, the Chief Information Officer (CIO), the senior leadership, and employees at all levels of the Department. The CIO accepts all of the recommendations in this report and remediation actions will include short, medium and long-term initiatives. We continue to focus on monitoring, detecting, remediating and inspecting all of our Information Technology (IT) systems, whether externally facing or internal, while instituting new capabilities to improve security around access and authentication, and data protection.

The mission of the Department of the Interior (Department) is broad with over 2,400 operating locations spanning the United States and its territories. Over 70,000 employees and more than 280,000 volunteers carry out the Department's mission serving communities large and small. They deliver the Department's land, energy, science, and community-based programs in ways that engage the participation of citizens, groups and businesses. The Department's current IT management structure reflects the decentralized nature of its programs and functions. The Department's Office of the Chief Information Officer (OCIO) is responsible for operation of Departmental systems and issues IT policy, while bureaus and offices are each responsible for their respective systems. The Department's OCIO is also responsible for reporting IT security incidents to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) and for relaying reports from US-CERT to bureaus/offices for appropriate action. In addition, the Department maintains an Advanced Security Operations Center (ASOC) with advanced tools to monitor network traffic and perimeter activity for the wide area network (WAN), which the bureaus/offices can leverage.

As demonstrated by the recent Office of Personnel Management (OPM) incident and the Office of Inspector General (OIG) Report, the risks and impacts of intrusions and compromise is high. Each week, the Department detects and prevents between five and six million malicious connection attempts to exploit vulnerabilities in its Internet perimeter and Internet facing systems. The CIO is working in partnership with the Department's senior leadership and the bureau/office experts to improve our ability to manage the risk of cyber-attacks while delivering the Department's mission.

On June 23, 2015, the Department's CIO convened a Cyber Security Advisory Group that includes representatives from the bureaus and the OCIO with expertise in a variety of IT and management disciplines. The Advisory Group will support the CIO in developing a strategy and action plan for the Department. This plan will be a comprehensive, multi-pronged approach to strengthen cyber security and privacy, and will address all of the recommendations in this Report, as well as the lessons learned from the OPM incident.

In implementing the requirements of the Federal Information Technology Acquisition Reform Act (FITARA) and the Federal Information Security Modernization Act (FISMA), the Department will adopt a more centralized approach to managing IT across the Department. FITARA strengthens CIO authorities in IT planning, budget, acquisitions and accountability over IT leaders in bureaus/offices. To meet FISMA requirements, the

Department will obtain access and visibility into the entire Department network and will play a more direct role in incident response working with its bureaus/offices and with US-CERT.

The Department's IT Transformation initiative, launched in December 2010 with the issuance of Secretarial Order 3309, Information Technology Management Functions and Establishment of Funding Authorities, called for the consolidation of commodity IT functions under the Department CIO. Our IT Transformation gave the Department a head start in consolidating and centralizing the management of IT infrastructure resources. As a result of this, DOI achieved the following:

- Improved cyber security capabilities using the Continuous Diagnostics and Mitigation (CDM) investment funded by Congress through DHS. Through this investment, DOI deployed continuous monitoring capabilities across the enterprise to DOI computing devices, including laptops, desktops, and servers. This gives the Department visibility into the vast majority of IT hardware and software assets on our network. Our CDM tools also give us the opportunity to centrally manage vulnerability patching at the Department level, which will greatly improve cyber hygiene across our IT landscape.

- Based on FISMA requirements, implemented strong authentication for all privileged users across the Department as of June 26, 2015. The Department is on track to meet the goal of implementing two-factor authentication for 75% of our unprivileged users by July 15, 2015. Two-factor authentication provides strong controls to ensure that only authorized users, whether a system administrator, or regular end-user, are able to gain access to DOI's IT systems. This protects us from intruders who can easily compromise usernames and passwords to gain access to our network.

- Consolidated 14 disparate email systems and moved more than 70,000 employees to a single, cloud-based email and collaboration system, known as BisonConnect. Implemented a separate, but integrated cloud-based electronic document and records management system to support the electronic journaling of emails. Reducing the number of duplicative email systems with different security policies and configurations helped the Department to shrink the threat surface around our email systems, enforcing a standard that we can more effectively and efficiently secure.

- Awarded a set of contracts to support our move to the cloud and moved our first major application, the Financial and Business Management System (FBMS), a customized SAP application, to the cloud. To support the Federal CIO's "Cloud First" Strategy, DOI has implemented a Mandatory Use Policy for the Foundation Cloud Hosting Services Contract requiring all bureaus/offices to evaluate cloud services first when refreshing technologies or standing up new initiatives. As of July 2015, DOI has awarded 15 cloud hosting contract task orders for internal and external customers. This provides the Department access to state-of-the-art, commercial "infrastructure-as-a-service (IAAS), platform-as-a-service (PAAS) and software-as-a-service (SAAS)" offerings that are FedRamp compliant. The cloud provides a

flexible, scalable, cost-effective and secure environment for hosting DOI's applications and data. We see the cloud as a pivotal part of our long-term future.

- Launched DOI's data center consolidation plan to support the OMB Federal Data Center Consolidation Initiative (FDCCI). Since 2011, DOI has consolidated 127 DOI data centers, exceeding DOI's initial commitment of 95 data centers. In addition, six DOI data centers have been categorized as core data centers, which will be leveraged as internal hosting consolidation points in addition to cloud and third-party options. Data center consolidation reduces the Department's IT footprint overall and provides us with internal hosting options for systems that are not yet cloud-ready. Consolidating smaller, non-core data centers into DOI's larger and more robust core data centers allows us to more efficiently and effectively manage and protect high value data.

Attachment 3

Office of the Chief Information Officer
Statement of Actions to Address Office of Inspector General Draft Evaluation Report Security of the U.S. Department of the Interior's Publicly Accessible Information Technology Systems Report No. ISD--IN--MOA--0004--2014

Recommendation 1: Require and enforce the secure development and management of all publicly available IT services, to include:

a. An official approval process;
b. Cloud candidacy evaluation;
c. Testing requirements;
d. Architectural designs and data flow;
e. Minimum layered security controls; and
f. Standardized platforms and utilities.

Response: The Department's Office of the Chief Information Officer (OCIO) accepts the finding and accompanying recommendation. The Chief Information Officer (CIO) will work with the Cyber Security Advisory Group to develop policy, plans and processes that consolidate all publicly accessible systems in a centrally managed demilitarized zone (DMZ) and/or cloud infrastructure. This will include implementing the architecture and defining the criteria for approval before web services, applications, and content "go live." Additionally, within 60 days, the OCIO will establish hardening requirements for environments housing publicly facing web sites and services for immediate implementation.

Responsible Official & Title: Sylvia Burns, Chief Information Officer
Initial Lead Contact & Title: Andrew Havely, Director Solution Design and Innovation
Target Completion Date: Resources permitting, the CIO will review alternatives for designing secure, consolidated DMZ architectures and the Department will adopt and implement the recommended public-facing web services architecture(s), by September 30, 2017.

Recommendation 2: Perform periodic discovery activities and reconcile results with approved inventory of Bureau and Department services to include:

a. all service site URLs;
b. all public IP ranges; and
c. identification of public systems housing sensitive or mission- critical data. (data call)

Response: The Department's OCIO accepts the finding and accompanying recommendation. The OCIO maintains an inventory of .GOV domain names registered to the Department and its bureaus and offices. The OCIO also maintains an inventory of public Internet Protocol (IP) address space owned and operated by the Department. The OCIO will validate and document the inventory of all web sites and services and their associated IP addresses including .GOV and other domain names DOI hosts on behalf of other agencies/entities.

The CIO will work with the Cyber Security Advisory Group to develop and implement policy and procedures that notify OCIO when a public facing system is approved to "go live." This

action builds on the policy, process, and procedures described in Recommendation 1. The OCIO will conduct additional periodic scanning of Internet facing systems and services to identify any discrepancies from known baseline and revise the inventory accordingly.

Responsible Official & Title: Sylvia Burns, Chief Information Officer
Initial Lead Contact & Title: Jerry Johnston, Director, Information and Technology Management
Target Completion Date: Pending availability of resources, September 30, 2017.

Recommendation 3: Expand existing external vulnerability scanning services to include the following:

a. advanced service exploit testing;
b. advance website (URL- based) exploit testing;
c. oversight of remediation activities to include;
    i. develop and enforce guidelines for mitigation timeliness that comply with DHS Binding Operational Directive 15-01;
    ii. tracking and validation of implemented solutions;
    iii. all external weakness identified by Bureaus, OCIO, OIG, or other third parties; and
d. trend analysis.

Response: The Department's OCIO accepts the finding and accompanying recommendation. Cyber vulnerabilities are discovered daily. For the best trend analysis and vulnerability scanning, the CIO will explore options to obtain third party support for trend analysis and technical exploit (advance service exploit testing) and penetration testing of both new and existing web sites and services.

Responsible Official & Title: Sylvia Burns, Chief Information Officer
Lead Contact & Title: Al Foster, Chief Information Assurance Operations
Target Completion Date: Pending availability of resources, September 30, 2016.

Recommendation 4: Require all publicly available systems to be hosted in an isolated infrastructure.

Response: The Department's OCIO accepts the finding and accompanying recommendation. The Department will implement technical controls to properly isolate systems and data that are exposed to the public as appropriate, segmenting these from the general corporate network. Within 60 days, the OCIO will issue a DMZ standard for immediate implementation across the Department. Ultimately, the Department will pursue a consolidated DMZ service.

Responsible Official & Title: Sylvia Burns, Chief Information Officer
Lead Contact & Title: Andrew Havely, Director, Solutions Design and Innovation and Stu Mitchell, Chief Network Architect
Target Completion Date: Resources permitting, by September 30, 2017.

Recommendation 5: Perform periodic advanced testing to validate the effectiveness of controls in isolating public systems from internal systems.

Response: The Department's OCIO accepts the finding and accompanying recommendation. The testing described in Recommendation 3 will include both external vulnerability scanning and advanced testing to ensure both new and existing public web sites and services are isolated from internal systems.

Responsible Official & Title: Sylvia Burns, Chief Information Officer
Lead Contact & Title: Al Foster, Chief, Information Assurance Operations
Target Completion Date: Resources permitting, by September 30, 2017.

Recommendation 6: Implement an intrusion monitoring solution that can analyze and correlate internal traffic patterns and detect attack signatures across Bureaus, including the capability for active traffic interception.

Response: The Department's OCIO accepts the finding and accompanying recommendation. Interior will implement additional technical controls to monitor internal network traffic and traffic flows, with a particular focus on the flow of traffic between isolated network segments containing publicly exposed systems and the general user network.

Responsible Official & Title: Sylvia Burns, Chief Information Officer
Lead Contact & Title: Al Foster, Chief Information Assurance Operations
Target Completion Date: September 30, 2016, resources permitting for the six Department Core Data Centers

All deletions have been made under 5 U.S.C. §§ 552(b)(6) and (b)(7)(C) unless otherwise noted

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

REPORT OF INVESTIGATION

Case Title [redacted]	**Case Number** **PI-PI-13-0457-I**
Reporting Office **Program Integrity Division**	**Report Date** **November 26, 2013**
Report Subject **Final Report of Investigation**	

SYNOPSIS

The Office of Inspector General received a complaint alleging that [redacted] Assistant Director for the Office of Law Enforcement and Security (OLES), Technology Division, had falsified his educational qualifications listed on the Department of the Interior Web site, as well as on LinkedIn.

Our investigation revealed that [redacted] obtained falsified university transcripts, claiming to have graduated with a master's degree from the University of Central Florida and a bachelor's degree from the University of Wisconsin-Oshkosh. We also determined that he made these claims on his official records he submitted to the Department of Interior.

We presented this case to the U.S. Attorney Office's for the District of Columbia and Maryland for possible violations of 18 USC 1001(False Statements) and 18 USC 1343 (Mail Fraud and Wire Fraud). The case was declined. On July 5, 2013, [redacted] resigned from the Department of the Interior.

DETAILS OF INVESTIGATION

On July 2, 2013, we received a complaint alleging that [redacted] Assistant Director for the Office of Law Enforcement and Security (OLES) Technology Division, falsified his educational background. The complainant said she found the information on the Department of the Interior (DOI) OLES Web site, as well as on LinkedIn. A subsequent interview with [redacted] analysis of his government computer, and our review of his personnel records indicated that he had obtained falsified transcripts. These records made it appear that he had a master's degree from the University of Central Florida and a bachelor's degree from the University of Wisconsin-Oshkosh **(Attachment 1 and 2)**. He submitted these records to Bureau of Safety and Environmental Enforcement (BSEE) Human Resources Division

Reporting Official/Title [redacted] Special Agent	Signature
Approving Official/Title [redacted] DAIG, Office of Investigations	Signature
Authentication Number: 158FA4B128056255581247263CFD33E5	

This document is the property of the Department of the Interior, Office of Inspector General (OIG), and may contain information that is protected from disclosure by law. Distribution and reproduction of this document is not authorized without the express written permission of the OIG.

All deletions have been made under 5 U.S.C. §§ 552(b)(6) and (b)(7)(C) unless otherwise noted

for his Government Official Personnel Folder (OPF). He cited both degrees on the resume he submitted to apply for the Senior Executive Service (SES) **(Attachment 3)**.

We interviewed the complainant, [redacted] University of Central Florida (UCF), Alumni Association **(Attachment 4)**. [redacted] said she first encountered references to [redacted] when trying to find UCF alumni living in the Washington, DC, area to whom she could introduce the UCF president during a future visit to Washington, DC. [redacted] said she searched the social media website, LinkedIn, where she found [redacted] profile. The profile indicated that he attended UCF between 1991 and 1993, receiving a master's degree in Technology Management **(Attachment 5)**.

[redacted] said she asked to join [redacted] "network." Initially, he accepted her request, but later deleted her from his network. Finding his response unusual, [redacted] searched UCF's alumni database, but could not find [redacted] listed. She then asked the registrar to search university records. The registrar's search indicated that [redacted] never attended UCF. The UCF registrar's office also confirmed these findings for OIG **(Attachment 6)**.

[redacted] LinkedIn profile also claimed that he attended the University of Wisconsin-Madison between 1986 and 1990, receiving a bachelor's degree in Information Technology (See Attachment 6).

Agent's Note: *The University of Wisconsin-Oshkosh is a part of the University of Wisconsin educational system. The University of Wisconsin-Madison is the main campus, located in a different part of the state.*

When we interviewed [redacted] about his education, [redacted] said he went to the University of Wisconsin-Oshkosh, "for a few years," starting in 1986, but had a break in studies after 1988 **(Attachment 7 and 8)**. He eventually left the university in 1989 without obtaining a bachelor's degree. [redacted] subsequently admitted that the only formal education he had received was through the Senior Executive Fellows Program at the Harvard Kennedy School, which OLES paid for after he joined DOI. When asked why he claimed to have a master's degree from UCF on his LinkedIn profile, [redacted] said, "I just…wanted to be something I'm not, I guess."

When asked if he claimed he had a master's degree from UCF anywhere else other than LinkedIn, [redacted] said he had told several of his friends and also posted it on his Facebook page. He later admitted that his resume also reflected that he had a master's degree. He insisted, however, that he did not claim to have a bachelor's degree on his SF-86 (Questionnaire for National Security Positions) and that he was positive he had not misrepresented his educational background on any official Government document.

When shown his official Federal Personal Payroll System (FPPS) data sheet that indicated he had a master's degree from UCF, [redacted] admitted requesting that his SF-50 (Notification of Personnel Action) be changed possibly 1 ½ years before **(Attachment 9)**. He admitted that his actions were wrong, claiming he did not know why he did it. [redacted] said that he provided Human Resources with false documentation of his UCF degree, which he had purchased from a fraudulent college transcript Web site.

A review of [redacted] OLES laptop revealed a fraudulent UCF master's degree transcript and a fraudulent University of Wisconsin-Oshkosh bachelor's degree transcript. We also recovered several

All deletions have been made under 5 U.S.C. §§ 552(b)(6) and (b)(7)(C) unless otherwise noted

emails indicating that [redacted] had contacted BSEE Human Resources Division on July 27, 2010 **(Attachment 10)**. During several email exchanges, [redacted] indicated that an error concerning his educational level had been made on his SF-50, citing that, although he had submitted transcripts when employed by DOI, only those pertaining to his bachelor's degree were used, rather than both his bachelor's and master's degrees. The human resources specialist replied that his SF-50 only showed transcripts for his bachelor's degree. A review of [redacted] OPF indicated that as of December 9, 2007, his hiring date, his educational level was a 13, equivalent to a bachelor's degree (See Attachment 9).

We contacted Human Resources for copies of the documents [redacted] submitted when applying for his DOI position. Human Resources could not find a copy of the initial vacancy announcement, but were able to locate the bachelor's degree transcript **(Attachment 11)**.

SUBJECT(S)

[redacted] Assistant Director for the Office of Law Enforcement and Security (OLES), Technology Division.

DISPOSITION

Case closed within PI.

ATTACHMENTS

1. Fraudulent University of Central Florida master's degree transcript.
2. Fraudulent University of Wisconsin-Oshkosh bachelor's degree transcript.
3. Resume package for OLES Senior Executive Service (SES).
4. IAR – Interview of [redacted] on July 2, 2013.
5. Copy of [redacted] LinkedIn profile.
6. Email from [redacted], Assistant University Registrar, University of Central Florida.
7. IAR – Interview of [redacted] on July 2, 2013.
8. Transcript of interview with [redacted] on July 2, 2013.
9. [redacted] Federal Personnel/Payroll system data sheet.
10. [redacted] emails regarding "SF-50 correction."
11. Office of Personnel Management certification of Investigation.

Colleen M. Kelley

National President

National Treasury Employees Union

Statement for the Record

For

Subcommittee on Information Technology and Subcommittee on Interior

House Committee on Oversight and Government Reform

"CYBERSECURITY: THE DEPARTMENT OF THE INTERIOR"

July 15, 2015

1750 H Street, N.W. • Washington, D.C. 20006 • (202) 572-5500

Chairman Hurd, Chairman Lummis, Ranking Member Kelly, and Ranking Member Lawrence, distinguished members of the Subcommittee on Information Technology and Subcommittee on Interior, I would like to thank you for the opportunity to share our members' perspectives on the recent Office of Personnel Management (OPM) data breaches impacting federal employees. I also commend you for holding this hearing regarding the Department of Interior's (DOI) role with federal employee personnel records and human resources functions and for devoting attention to this extremely urgent issue. As President of the National Treasury Employees Union (NTEU), I have the honor of representing over 150,000 federal workers in 31 agencies.

There is still great fear and outrage on the part of federal employees and retirees in the aftermath of OPM's recent announcements that millions of current and former federal employees have had personally identifiable information (PII) compromised owing to breaches in databases containing various personnel and investigative records. Federal employees have had a difficult few years, facing multi-year pay freezes, furloughs, sequestration, and this type of exposure is simply unacceptable.

Following its first statements beginning on June 4th, OPM confirmed that a personnel records breach had potentially compromised names, dates and places of birth, Social Security numbers, and addresses. A month later, much remains unknown about what type of personnel records were compromised, making it impossible for these 4.2 million federal employees and retirees, to truly understand the risk that they, and possibly their family members, are facing. Employees deserve to know what exact databases and information was hacked, particularly given the high number of OPM databases that exist containing various types of agency and employee records.

Media reports have indicated that the Interior Business Center (IBC), a unit of DOI, which serves as a shared services provider for a number of federal agencies, responsible for a myriad of human resources, financial, payroll, data warehouse, and benefits administration functions, may have been involved in the OPM personnel records breach. Additionally, IBC also provides support for the Office of Management and Budget's and OPM's Human Resources Line of Business (HRLoB), that seeks to modernize, align, and allow for strategic human capital planning in the day-to-day management of employing agency human resources functions and processes. Further, recent congressional hearings on the OPM breaches have confirmed that the electronic Official Personnel Folder system (eOPF), one of OPM's key e-government initiatives under the Enterprise Human Resources Integration (EHRI) initiative, that aims to consolidate, gather, and transform the use of government-wide data and human resources processes though the use of information technology, was compromised. While much attention has focused on OPM in recent weeks, it is important to remember that all federal agencies, including DOI, house huge amounts of personal information on the federal workforce, as well as for many other Americans. Congress needs to ensure that agencies receive the proper funding to be able to adequately safeguard this information physically and virtually, and to hire and retain a skilled IT workforce.

Given IBC's various roles for federal agencies, NTEU believes additional information is needed as to what exact data and personal information was compromised, including whether or

not any of the personnel records contained family member information, such as would occur for family member benefit designations for the Federal Employees Health Benefits Program (FEHBP) or the Federal Employees Group Life Insurance (FEGLI) program. IBC's payroll functions also lead to serious remaining questions as to the security of employee's financial and bank account information. I ask Members of the Committee on Oversight and Government Reform to ensure that affected federal employees and retirees know for sure what was and was not compromised in the personnel records breach. While the U.S. government cannot now undo the damage caused by the breach, it can at least be transparent about the data compromised, and duly inform affected employees and retirees.

NTEU continues to seek notifications for individuals affected by the background investigations breach, who a month following its announcement, have yet to be notified. These individuals have given the U.S. government the most sensitive personal information that exists, and deserve to have credit and identity theft protections already in place. We are also working to ensure free lifetime credit monitoring, including the option to set up credit freezes, as well as free lifetime identity theft protection for affected individuals, and support Congresswoman Eleanor Holmes Norton's bill, *H.R. 3029*. I ask that your Subcommittees support this legislation, and seek swift passage of this measure by the U.S. House of Representatives. I also urge your Subcommittees to ensure the creation of a high level task force to quickly secure personnel databases across government, and to seek a review of what information the federal government requires employees, and their family members, to provide, and how agencies collect, process, disseminate, and store this information. And, further to review the Executive branch's "Continuous Evaluation" (CE) proposals which would expand the amount of personal information gathered for those serving in sensitive positions in light of these recent data breaches.

Thank you for the opportunity to share NTEU's views.

Statement of Congressman Gerald E. Connolly (VA-11)
Joint Hearing of the Subcommittees on Information Technology & Interior
Cybersecurity: The Department of the Interior
July 15, 2015

The devastating series of data breaches perpetrated against U.S. Office of Personnel Management (OPM) databases represent one of the most catastrophic compromises of sensitive personally identifiable information (PII) in our Nation's history. The United States Government failed to protect its most valuable asset – the millions of dedicated Federal workers, Federal retirees, and contract personnel that serve our country with honor and distinction.

I recall how arduous, intrusive, and time-consuming it was to complete the comprehensive "Questionnaire for National Security Positions" – which was necessary to obtain the top secret security clearance I required to carry out my staff duties on the Senate Foreign Relations Committee. And as any individual who has undergone a background investigation to gain access to classified material understands, the sensitive PII contained in each of these comprehensive questionnaires that exceed 100 pages in length, constitutes a veritable treasure trove of information that any foreign intelligence service would consider incredibly valuable.

Taken in totality, the sophisticated intrusions at OPM that compromised the PII of millions of federal employees and clearance holders and the subsequent breach of the U.S. Department of Interior's (DOI) data center that hosted OPM's Central Personnel Data File (CPDF) raise highly troubling questions over the emerging threat posed by a foreign adversary in possession of a detailed dossier on the entire Federal workforce, and millions of deeply personal records pertaining to our national security personnel.

As a Member who has the privilege of representing tens of thousands of dedicated civil servants and contract personnel, I share my constituents' outrage over the collective failure of agencies and covered contractors to prevent repeated intrusions into Federal networks; to mitigate the damage caused by attackers that breach network perimeters; and to provide individuals whose PII has been compromised clear, timely, and accurate information on the incident and the steps that are being taken to limit the harm.

My constituents still have many unanswered questions and unresolved concerns relating to the series of massive data breaches. In particular, the public still does not fully understand why DOI established an interagency agreement with OPM to house and presumably safeguard the CPDF in the first place, let alone why DOI allowed its data center, which must have been accredited as a high-impact level system under the Federal Information Security Management Act (FISMA), to be breached. That is why today's hearing is so important. Without discounting the critical national security catastrophe of compromising millions of background investigation documents; Congress must not overlook or ignore the CPDF data breach, which alone resulted in the loss of PII for more than 4 million Federal employees and retirees.

This incident raises important policy questions over the Federal Government's continued insistence on remaining in the business of owning and operating data centers; the consequences of our government's stubborn cultural resistance to embracing advanced commercial cloud computing solutions; and the danger posed by confederated agencies characterized by disparate silos, with no central authority over information technology policy. This last issue appears to be a recurring theme, as the DOI Office of Inspector General (OIG) is now the second OIG to

testify before this Committee that an agency's failure to effectively centralize policy, guidance, and enforcement with its Office of Chief Information Officer (OCIO) was a key factor that undermined its cybersecurity capabilities and readiness.

On a positive note, it does appear that the recent massive data breaches may finally be the proverbial straw that breaks the camel's back. As the DOI CIO testified at our June 16, 2015 Committee hearing, the Secretary of the Interior has directed her office "...to take the lead in mitigating critical vulnerabilities for all of DOI's IT systems" as part of a broader action plan.

However, it is clear much work remains to be done across the Federal Government. Fortunately, with the December 2014 enactment of the Federal Information Technology Acquisition Reform Act (FITARA), implementing IG recommendations to enhance an agency's CIO authorities has been elevated from a simple administrative best practice to clear statutory requirement. As the Department of Homeland Security's former Chief Human Capital Officer recently wrote in an op-ed published by The Washington Post:

"The harm that parochial culture can cause grows as our systems become more complex and more interconnected. In fact, correcting that cultural flaw is one of the primary objectives of the Federal Information Technology Acquisition Reform Act (FITARA). FITARA will give Department Chief Information Officers much greater control over such programs. The result should be a focus on security throughout the acquisition, development and deployment processes."

Moving forward, Congress and the Administration must work together in a pragmatic and urgent fashion to ensure that the right statutory framework is in place to combat threats posed by cyber adversaries, and that agencies follow through in swiftly acquiring and deploying the most advanced information security defenses, such as Einstein 3 Accelerated and Continuous Diagnostics and Mitigation program tools and services. America needs to embrace a "whole of government" approach that focuses on mastering basic cyber hygiene. While the Administration's launch of a 30 day cyber sprint was better late than never, I regret that it took such a calamitous breach to force action on priorities that the Office of Management and Budget has been pushing agencies to adopt for years, across multiple Administrations.

The bottom line is that the race to harden America's cyber defenses is more aptly compared to a never-ending marathon than a quick sprint. Whether dealing with people, specifically recruiting and retaining the next generation of cybersecurity professionals; addressing policy, such as authorizing information sharing, security standards, and cyber integration centers; or practices, in this case making good cyber hygiene as much of a social norm as washing one's hands after using the restroom; our Nation remains in the nascent stages of strengthening cybersecurity.

Today's hearing is an important step in furthering our efforts to proceed in the most informed manner possible as we look to ensure that the Federal Government dramatically strengthens its cyber security defenses and private sector vendors utilize the best information security practices to protect our constituents' sensitive PII and defend our national security interests at home and abroad.

Office of the Inspector General, U.S. Department of the Interior Report:

SECURITY OF THE U.S. DEPARTMENT OF THE INTERIOR'S PUBLICLY ACCESSIBLE INFORMATION TECHNOLOGY SYSTEMS

Report No. : ISD-IN-MOA-0004-2014

July 2015

Available at: https://www.doioig.gov/sites/doioig.gov/files/ISDINMOA00042014Public.pdf

○