GAO HIGH RISK FOCUS: CYBERSECURITY

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

AND THE

SUBCOMMITTEE ON
GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

————

JULY 25, 2018

————

Serial No. 115–110

————

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana
Michael Cloud, Texas

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
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Jimmy Gomez, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Stacey E. Plaskett, Virgin Islands
John P. Sarbanes, Maryland

SHERIA CLARKE, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
MEGHAN GREEN, *Counsel*
TROY STOCK, *Information Technology Subcommittee Staff Director*
JULIE DUNNE, *Government Operations Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

Will Hurd, Texas, *Chairman*

Paul Mitchell, Michigan, *Vice Chair*
Darrell E. Issa, California
Justin Amash, Michigan
Steve Russell, Oklahoma
Greg Gianforte, Montana
Michael Cloud, Texas

Robin L. Kelly, Illinois, *Ranking Minority Member*
Jamie Raskin, Maryland
Stephen F. Lynch, Massachusetts
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

Mark Meadows, North Carolina, *Chairman*

Jody B. Hice, Georgia, *Vice Chair*
Jim Jordan, Ohio
Mark Sanford, South Carolina
Thomas Massie, Kentucky
Ron DeSantis, Florida
Dennis A. Ross, Florida
Rod Blum, Iowa

Gerald E. Connolly, Virginia, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey

C O N T E N T S

GAO HIGH RISK FOCUS: CYBERSECURITY

Wednesday, July 25, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY joint
WITH SUBCOMMITTEE ON GOVERNMENT OPERATIONS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:25 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the Subcommittee on Information Technology] presiding.

Present: Representatives Hurd, Mitchell, Hice, Amash, Massie, DeSantis, Blum, Kelly, Connolly, Raskin, Maloney, and Norton.

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

I would like to now recognize my friend and partner in crime, the distinguished gentlewoman from the great State of Illinois, for her opening remarks.

Ms. KELLY. Thank you, Mr. Chair. And not too much crime.

Thank you, Mr. Chairman and Chairman Meadows, for holding this important hearing. Ms. Kent, welcome to today's hearing, and thank you for testifying today and sharing your vision for cybersecurity as a new Federal COI, and it's great to meet you in my office.

And, Mr. Dodaro, special thanks to you for the extensive work you and all the dedicated professionals at GAO put into providing this special midcycle high-risk report on cybersecurity, and it was nice meeting with you also.

GAO's newly issued report raises serious concerns about our Nation's ability to confront cybersecurity risk. GAO found key deficiencies that could hinder the government's progress in strengthening the Nation's cyber defenses. For example, GAO found that the Trump administration's plans failed to include basic components needed to carry out a national strategy for protecting critical cyber infrastructure.

Among the missing components were details about performance measurements and milestones for determining whether the country's cyber objectives are being met and the resources that would be needed to carry out those objectives. GAO's report highlights the need for the administration to develop and execute a more comprehensive Federal strategy for national cybersecurity and global cyberspace. It underscores the importance of having a cybersecurity

coordinator in the White House to develop a more robust cybersecurity strategy for the country.

But, here again, the Trump administration is not rising to the challenge. Two months ago, the President's National Security Advisor, John Bolton, eliminated the position of White House cybersecurity coordinator. This decision was contrary to a prior GAO recommendation to have a White House cybersecurity coordinator in the Executive Office of the President develop an overarching Federal cybersecurity strategy at a time when our Nation is facing persistent cyber threats ranging from foreign adversaries who seek to undermine our elections to criminal hackers who steal sensitive data. The administration's decision to eliminate the key cybersecurity position in the White House should raise alarm.

Today's report also shows that the number of Americans whose personal information has been compromised and government and private sector data breaches is growing. And there's a need for stronger measures and congressional action to protect consumer privacy. GAO found that the vast number of individuals potentially affected by data breaches at Federal agencies and private sector entities in recent years increases concerns that personally identifiable information is not being properly protected.

GAO's findings is supported by two recent reports that highlight the heightened, challenged public and private sector organizations are facing in securing sensitive data. In April, Verizon issued a report showing that in the past 12 months alone, there with over 53,000 incidents and 2,216 confirmed data breaches. And just last week, the Attorney General's Cyber-Digital Task Force released a report showing that there were at least 686 data breaches reported in the first quarter of 2018, resulting in the theft of as many as 1.4 billion records.

Last year, data breaches at Equifax in which over 143 million Americans had their personal information stolen and the 2015 breach at OPM, which affected approximately 22.1 million individuals, illustrates the massive scale of harm to privacy and security that these breaches have. To address the growing concerns about privacy, GAO recommended that Congress straighten out privacy laws, the majority of which were written well before the development of new technologies, ranging from the use of social networking sites, the facial recognition technologies, and many mobile applications. Congress should heed GAO's recommendations and reexamine how our privacy laws can be strengthened to ensure that consumers' personal privacy is adequately protected.

I want to thank our witnesses for testifying today. And I normally would say I look forward to hearing your testimony, but I have to leave. But I look forward to reading it on how we can improve the Nation's cybersecurity.

And thank you again, my friend, Mr. Chairman.

Mr. HURD. Good afternoon, y'all. Today's hearing returns to a familiar field for this subcommittee, an area of top bipartisan concern and focus, and that's the cybersecurity of the Federal Government. The Federal Government and our Federal agencies, like everything else in today's digital society, are dependent on IT systems and electronic data, which make them highly vulnerable to a wide and evolving array of cyber threats.

Federal civilian agencies report over 35,000 information security incidents to the US–CERT last fiscal year. This represents a 14 percent increase over the previous year. Securing Federal systems and data is vital to the Nation's security, prosperity, and well-being. It should concern all of us, therefore, that the GAO has concluded in the interim high-risk report, that spurred this hearing, that urgent actions are needed to address ongoing cybersecurity challenges in the Federal Government.

In this report, the GAO identified four major cybersecurity challenges: establishing a comprehensive cybersecurity strategy in performing effective oversight, securing Federal systems and information, protecting cyber critical infrastructure, and protecting privacy and sensitive data. To address these four challenges, GAO identified 10 critical actions the Federal Government entities need to take. I'm looking forward to exploring those 10 items.

Since 2010, GAO has made over 3,000 recommendations to agencies aimed at addressing these four cybersecurity challenges. And as of June of this year, nearly 1,000 of those recommendations have not been implemented. It's not acceptable given the threat we face. These open, lingering vulnerabilities put us at incredible risk, as we saw with the devastating data breaches at OPM.

While I do not expect Ms. Kent or anyone else to have all the answers today, I want to hear from GAO, the most critical open recommendations, and from Ms. Kent, concrete plans to close them. I want to commend Mr. Dodaro and his team at GAO for issuing this report. Midcycle updates to the high-risk list are not common. I recommend all agency CIOs read this report and apply the applicable recommendations to the respective agencies and systems, because guess what, we're going to be asking you about them.

And, as always, I'm honored to explore these issues in a bipartisan fashion with Ranking Member Kelly, Chairman Meadows, and Ranking Member Connolly. The four of us have worked together for years on these issues, and I'm honored to be joined here with them throughout today's hearing.

Now, it's a pleasure to introduce our witnesses. The Honorable Gene Dodaro, comptroller general of the United States Government Accountability Office. You always hold a special place in my heart because you were my first hearing being in Congress. Mr. Dodaro is accompanied by Mr. Gregory C. Wilshusen, the director of Information Security Issues at GAO, who will also be sworn in. And Ms. Suzette Kent, Federal chief information officer at the Office of Management and Budget. I think this is your first time here. I don't think it's the first time testifying in Congress, but welcome.

Pursuant to committee rules, all witnesses will be sworn in before they testify. So please stand and raise your right hand.

Do you solemnly swear or affirm that the testimony you're about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Thank you.

Please let the record reflect that all witnesses answered in the affirmative.

And in order to allow time for discussion, please limit your testimony to 5 minutes. The entire written statement has been made part of the record. And as a reminder, the clock will show your

time remaining. When it's yellow, you have 30 seconds. When it's red, your time is up. And remember to press the button.

And we'll start with Mr. Dodaro. You're now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF GENE L. DODARO

Mr. DODARO. Thank you very much, Mr. Chairman, Ranking Member Kelly, members of the committees that are here today. I very much appreciate the opportunity to be here to discuss this important topic.

This is an area that's been of long concern to me. We at GAO designated cybersecurity across the Federal Government as a high-risk area in 1997. So nobody could say we didn't warn people that this was going to be a problem. In 2003, we expanded that high-risk designation to include critical infrastructure protection. And, in 2015, we included the need to protect personally identifiable sensitive information as well.

Now, the government has taken a number of actions, especially since the OPM breach. Mr. Chairman, as you mentioned, there's been executive orders, strategies, document studies, but there still needs—much more needs to be done in this area.

As you referenced in your opening statement, since 2010, we've made over 3,000 recommendations. While two-thirds of those have been implemented, there's still 1,000 recommendations that need action. Now, the four areas that we identified I think are especially important.

First is establishing a comprehensive strategy, and importantly, having effective mechanisms in place to oversee its effective implementation. And this is to include global supply chain issues; critical workforce issues; and in dealing with emerging technologies that are going to bring new risk, such as artificial intelligence, the internet of things, quantum computing.

Secondly, there needs to be more urgent action to secure the Federal information systems. There needs to be more effective implementation of governmentwide efforts like continuous diagnostics and mitigation. Agencies need to fix their systems. There needs to be more attention in responding effectively when incidents do occur. Over time, we've seen agencies be slow to implement the effective actions over times.

On critical infrastructure protection, and this is an area that needs a lot more Federal attention. Now, in many areas, the Federal Government has some regulatory responsibilities in this area, but by and large critical infrastructure protection is a voluntary effort by the private sector. The National Institutes of Standards and Technology have developed an approach that the private sector can use, but it's all voluntary. So there's really not a clear picture, in my opinion, across the different sectors. And there's 16 different sectors of the economy that make up critical infrastructure, including electricity grid, telecommunications, nuclear issues, utilities, et cetera, the financial market areas as well.

So these are vital to our economic health. They're vital to public health and safety. And there needs to be more collaboration and a

better understanding of to what extent have these voluntary standards been implemented by the various sectors, and what is their state of readiness to deal with these issues?

The fourth area deals with privacy. Now, here, Federal agencies themselves need to better secure sensitive information. We've issued reports recently on a need to protect Medicare beneficiary data, for example, electronic health information systems, data on Federal student loans, there's a lot of personal data there, financial data that families submit. So that needs to be dealt with definitely. And we need to think about what information the Federal Government will collect going forward. We've made some recommendations on need to eliminate unnecessary use of Social Security information, for example.

We also have recommendations to the Congress in this area. The Privacy Act that was passed in 1974. The Electronic Government Act was passed in 2002, they need updated as well. And I'd also—we've recommended, since 2013, that the Congress establish a consumer privacy framework for the private sector.

In those areas, the Federal Government has put out, in some sectors, healthcare and, you know, credit reporting, some requirements for the private sector. But by and large the Federal Government has not set requirements for this area, particularly as it relates to information resellers as well.

So, again, Mr. Chairman, I want to thank you for the opportunity to be here today. I asked our team to put together this special report because I don't think the Federal Government's moving at a pace commensurate with the evolving threat in this area, and we need all to work harder, faster to address this issue.

Thank you very much.

[Prepared statement of Mr. Dodaro follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, July 25, 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Statement of Gene L. Dodaro,
Comptroller General of the United States

GAO Highlights

July 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Why GAO Did This Study

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being.

The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

GAO was asked to update its information security high-risk area. To do so, GAO identified the actions the federal government and other entities need to take to address cybersecurity challenges. GAO primarily reviewed prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas. GAO also reviewed recent cybersecurity policy and strategy documents, as well as information security industry reports of recent cyberattacks and security breaches.

What GAO Recommends

GAO has made over 3,000 recommendations to agencies since 2010 aimed at addressing cybersecurity shortcomings. As of July 2018, about 1,000 still needed to be implemented.

What GAO Found

GAO has identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them. GAO continues to designate information security as a government-wide high-risk area due to increasing cyber-based threats and the persistent nature of security vulnerabilities.

Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges

Major challenges	Critical actions needed
Establishing a comprehensive cybersecurity strategy and performing effective oversight	Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
	Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
	Address cybersecurity workforce management challenges.
	Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
Securing federal systems and information	Improve implementation of government-wide cybersecurity initiatives.
	Address weaknesses in federal agency information security programs.
	Enhance the federal response to cyber incidents.
Protecting cyber critical infrastructure	Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).
Protecting privacy and sensitive data	Improve federal efforts to protect privacy and sensitive data.
	Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis. | GAO-18-645T

GAO has made over 3,000 recommendations to agencies aimed at addressing cybersecurity shortcomings in each of these action areas, including protecting cyber critical infrastructure, managing the cybersecurity workforce, and responding to cybersecurity incidents. Although many recommendations have been addressed, about 1,000 have not yet been implemented. Until these shortcomings are addressed, federal agencies' information and systems will be increasingly susceptible to the multitude of cyber-related threats that exist.

_____ United States Government Accountability Office

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees:

I appreciate the opportunity to be here today to participate in your hearing on cybersecurity challenges. Federal agencies and our nation's critical infrastructures[1]—such as energy, transportation systems, communications, and financial services—are dependent on information technology (IT) systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security, prosperity, and well-being.

Many of these systems contain vast amounts of personally identifiable information (PII),[2] thus making it imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents, when they occur. Underscoring the importance of this issue, we continue to designate information security as a government-wide high-risk area in our most recent biennial report to Congress—a designation we have made in each report since 1997.[3]

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. These risks include insider

---

[1]The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. §5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[3]See GAO, High-Risk Series: An Update, GAO-17-317 (Washington, D.C.: February 2017) and High Risk Series: An Overview, GAO-HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks.

In particular, foreign nations—where adversaries may possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks. Rapid developments in new technologies, such as artificial intelligence and the Internet of Things (IoT),[4] makes the threat landscape even more complex and can also potentially introduce security, privacy, and safety issues that were previously unknown.

Compounding these risks, IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. This is illustrated by significant security breaches reported by the Office of Personnel Management (OPM) in 2015 that resulted in the loss of PII for an estimated 22.1 million individuals and, more recently, in 2017, a security breach reported by Equifax—one of the nation's largest credit bureaus— that resulted in the loss of PII for an estimated 148 million U.S. consumers.

At your request, my testimony updates the information security high-risk area by identifying actions that the federal government and other entities need to take to address cybersecurity challenges facing the nation. This statement reflects work we conducted since the prior high-risk update was issued in February 2017, among other things.[5] We also plan to issue an updated assessment of this high-risk area in February 2019.

In conducting the work for this update, we first identified cybersecurity areas in which the federal government has experienced challenges. To do so, we primarily reviewed our prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity

---

[4]IoT refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.

[5]GAO-17-317.

incidents, among other areas (see appendix I for a list of our prior work). We also reviewed recent cybersecurity policy and strategy documents issued by the current administration, such as Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[6] the National Security Strategy,[7] and the Department of Homeland Security's (DHS) May 2018 cybersecurity strategy.[8] We then analyzed these documents to determine the extent to which they included GAO's desirable characteristics of a national strategy.[9] We also reviewed recent media and information security industry reports of cyberattacks and security breaches. Based on these actions, we identified four cybersecurity areas in which federal agencies had experience challenges.

To identify the actions needed to address each challenge area, we reviewed the findings of our work specific to each challenge, the status of our prior recommendations to the Executive Office of the President and federal agencies, and any actions taken by these entities to address our recommendations. In reviewing the status of prior recommendations, we also determined which recommendations had not been implemented and what additional actions, if any, the Executive Office of the President and federal agencies needed to take in order to address them. We then summarized the actions needed and the status of our prior recommendations. We also identified our ongoing work related to each action.

We conducted the work on which this testimony is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate

---

[6]Exec. Order No. 13800, 82 Fed Reg. 22391 (May 16, 2017).

[7]The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: Dec. 2017).

[8]DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018). DHS has broad authorities to improve and promote cybersecurity of federal and private-sector networks. Specifically, long-standing federal policy as promulgated by a presidential policy directive, executive orders, and the National Infrastructure Protection Plan have designated DHS as a lead federal agency for coordinating, assisting, and sharing information with the private-sector to protect critical infrastructure from cyber threats.

[9]In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

IT systems supporting federal agencies and our nation's critical infrastructures are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.

Compounding the risk, federal systems and networks are also often interconnected with other internal and external systems and networks, including the Internet. This increases the number of avenues of attack and expands their attack surface. As systems become more integrated, cyber threats will pose an increasing risk to national security, economic well-being, and public health and safety.

Advancements in technology, such as data analytics software for searching and collecting information, have also made it easier for individuals and organizations to correlate data (including PII) and track it across large and numerous databases. For example, social media has been used as a mass communication tool where PII can be gathered in vast amounts. In addition, ubiquitous Internet and cellular connectivity makes it easier to track individuals by allowing easy access to information pinpointing their locations. These advances—combined with the increasing sophistication of hackers and others with malicious intent, and the extent to which both federal agencies and private companies collect sensitive information about individuals—have increased the risk of PII being exposed and compromised.

Cybersecurity incidents continue to impact entities across various critical infrastructure sectors. For example, in its 2018 annual data breach investigations report,[10] Verizon reported that 53,308 security incidents and 2,216 data breaches were identified across 65 countries in the 12 months since its prior report. Further, the report noted that cybercriminals can often compromise a system in just a matter of minutes—or even

[10]Verizon, *2018 Data Breach Investigation Report-11th Edition*, April 2018.

seconds, but that it can take an organization significantly longer to discover the breach. Specifically, the report stated nearly 90 percent of the reported breaches occurred within minutes, while nearly 70 percent went undiscovered for months.

These concerns are further highlighted by the number of information security incidents reported by federal executive branch civilian agencies to DHS's U.S. Computer Emergency Readiness Team (US-CERT).[11] For fiscal year 2017, 35,277 such incidents were reported by the Office of Management and Budget (OMB) in its 2018 annual report to Congress, as mandated by the Federal Information Security Modernization Act (FISMA).[12] These incidents include, for example, web-based attacks, phishing,[13] and the loss or theft of computing equipment.

Different types of incidents merit different response strategies. However, if an agency cannot identify the threat vector (or avenue of attack),[14] it could be difficult for that agency to define more specific handling procedures to respond to the incident and take actions to minimize similar future attacks. In this regard, incidents with a threat vector categorized as "other" (which includes avenues of attacks that are unidentified) made up 31 percent of the various incidents reported to US-CERT. Figure 1 shows the percentage of the different types of incidents reported across each of the nine threat vector categories for fiscal year 2017, as reported by OMB.
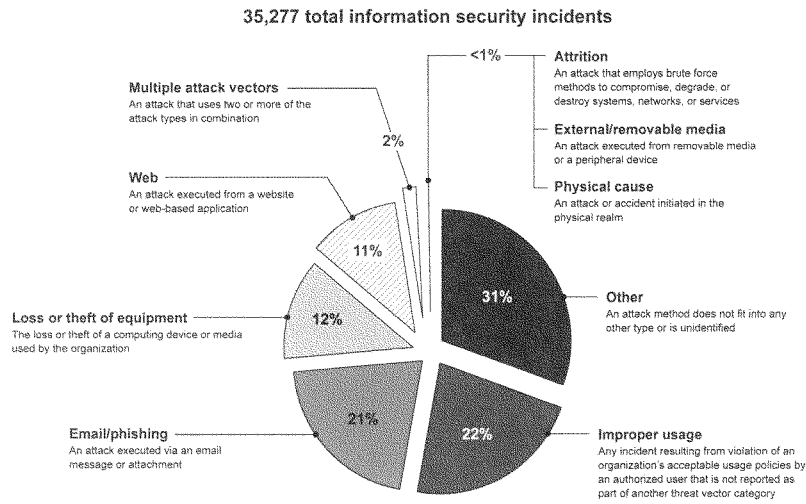
---

[11]US-CERT, a branch of DHS's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

[12]The Federal Information Security Modernization Act of 2014 was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code.

[13]Phishing is a digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.

[14]A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack. US-CERT's Federal Incident Notification Guidelines specify nine potential attack vectors agencies should use to describe incident security incidents during reporting.

Figure 1: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2017

35,277 total information security incidents

Multiple attack vectors
An attack that uses two or more of the attack types in combination

Web
An attack executed from a website or web-based application

Loss or theft of equipment
The loss or theft of a computing device or media used by the organization

Email/phishing
An attack executed via an email message or attachment

Attrition
An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

External/removable media
An attack executed from removable media or a peripheral device

Physical cause
An attack or accident initiated in the physical realm

Other
An attack method does not fit into any other type or is unidentified

Improper usage
Any incident resulting from violation of an organization's acceptable usage policies by an authorized user that is not reported as part of another threat vector category

Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2017. | GAO-18-645T

These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security. The following examples highlight the impact of such incidents:

* In March 2018, the Mayor of Atlanta, Georgia reported that the city was victimized by a ransomware[15] cyberattack. As a result, city

---

[15]According to DHS, ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

government officials stated that customers were not able to access multiple applications that are used to pay bills or access court related information. In response to the attack, the officials noted that they were working with numerous private and governmental partners, including DHS, to assess what occurred and determine how best to protect the city from future attacks.

- In March 2018, the Department of Justice reported that it had indicted nine Iranians for conducting a massive cybersecurity theft campaign on behalf of the Islamic Revolutionary Guard Corps. According to the department, the nine Iranians allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 U.S. companies, and five federal government agencies, among other entities.

- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation (FBI)[16] stated that, since at least March 2016, Russian government actors had targeted the systems of multiple U.S. government entities and critical infrastructure sectors. Specifically, the alert stated that Russian government actors had affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors.

- In July 2017, a breach at Equifax resulted in the loss of PII for an estimated 148 million U.S. consumers. According to Equifax, the hackers accessed people's names, Social Security numbers (SSN), birth dates, addresses and, in some instances, driver's license numbers.

- In April 2017, the Commissioner of the Internal Revenue Service (IRS) testified that the IRS had disabled its data retrieval tool in early March 2017 after becoming concerned about the misuse of taxpayer data. Specifically, the agency suspected that PII obtained outside the agency's tax system was used to access the agency's online federal student aid application in an attempt to secure tax information through the data retrieval tool. In April 2017, the agency began notifying taxpayers who could have been affected by the breach.

- In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a

---

[16]The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. The agency's Cyber Division leads efforts to investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

separate, but related, incident had compromised its systems and the files related to background investigations for 21.5 million individuals. In total, OPM estimated 22.1 million individuals had some form of PII stolen, with 3.6 million being a victim of both breaches.

Federal Information Security Included on GAO's High-Risk List Since 1997

Safeguarding federal IT systems and the systems that support critical infrastructures has been a long-standing concern of GAO. Due to increasing cyber-based threats and the persistent nature of information security vulnerabilities, we have designated information security as a government-wide high-risk area since 1997.[17] In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure.[18] At that time, we highlighted the need to manage critical infrastructure protection activities that enhance the security of the cyber and physical public and private infrastructures that are essential to national security, national economic security, and/or national public health and safety.

We further expanded the information security high-risk area in 2015[19] to include protecting the privacy of PII. Since then, advances in technology have enhanced the ability of government and private sector entities to collect and process extensive amounts of PII, which has posed challenges to ensuring the privacy of such information. In addition, high-profile PII breaches at commercial entities, such as Equifax, heightened concerns that personal privacy is not being adequately protected.

Our experience has shown that the key elements needed to make progress toward being removed from the High-Risk List are top-level attention by the administration and agency leaders grounded in the five criteria for removal, as well as any needed congressional action. The five criteria for removal that we identified in November 2000 are as follows:[20]

---

[17]GAO-HR-97-1.

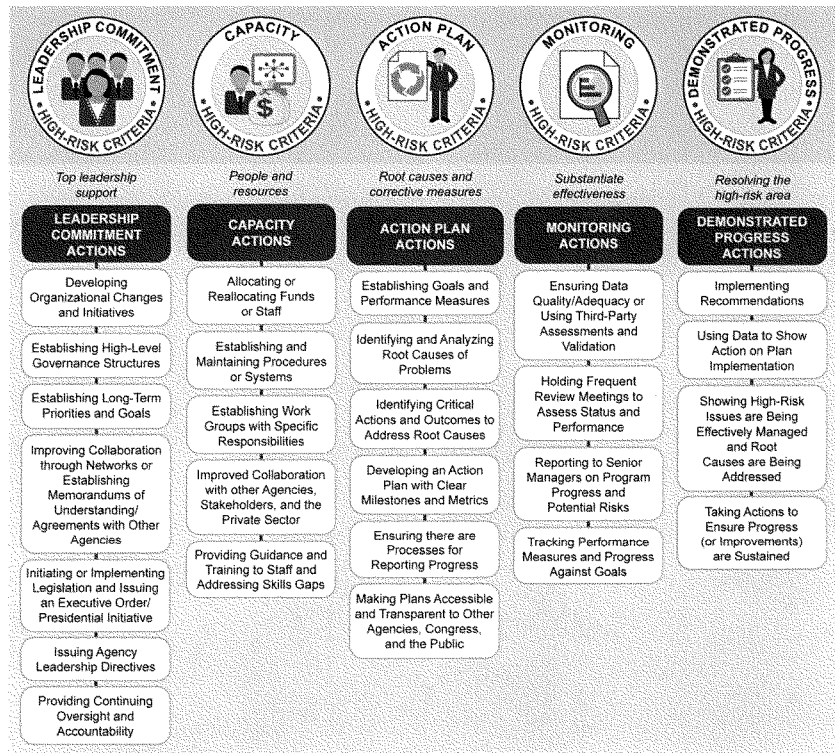[18]See GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

[19]See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

[20]GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

- **Leadership Commitment.** Demonstrated strong commitment and top leadership support.

- **Capacity.** The agency has the capacity (i.e., people and resources) to resolve the risk(s).

- **Action Plan.** A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions we recommended.

- **Monitoring.** A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.

- **Demonstrated Progress.** Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.

These five criteria form a road map for efforts to improve and ultimately address high-risk issues. Addressing some of the criteria leads to progress, while satisfying all of the criteria is central to removal from the list. Figure 2 shows the five criteria and illustrative actions taken by agencies to address the criteria. Importantly, the actions listed are not "stand alone" efforts taken in isolation from other actions to address high-risk issues. That is, actions taken under one criterion may be important to meeting other criteria as well. For example, top leadership can demonstrate its commitment by establishing a corrective action plan including long-term priorities and goals to address the high-risk issue and using data to gauge progress—actions which are also vital to monitoring criteria.

17

Figure 2: Criteria for Removal from the High-Risk List and Examples of Actions Leading to Progress

Top leadership support	People and resources	Root causes and corrective measures	Substantiate effectiveness	Resolving the high-risk area
LEADERSHIP COMMITMENT ACTIONS	**CAPACITY ACTIONS**	**ACTION PLAN ACTIONS**	**MONITORING ACTIONS**	**DEMONSTRATED PROGRESS ACTIONS**
Developing Organizational Changes and Initiatives	Allocating or Reallocating Funds or Staff	Establishing Goals and Performance Measures	Ensuring Data Quality/Adequacy or Using Third-Party Assessments and Validation	Implementing Recommendations
Establishing High-Level Governance Structures	Establishing and Maintaining Procedures or Systems	Identifying and Analyzing Root Causes of Problems		Using Data to Show Action on Plan Implementation
Establishing Long-Term Priorities and Goals	Establishing Work Groups with Specific Responsibilities	Identifying Critical Actions and Outcomes to Address Root Causes	Holding Frequent Review Meetings to Assess Status and Performance	Showing High-Risk Issues are Being Effectively Managed and Root Causes are Being Addressed
Improving Collaboration through Networks or Establishing Memorandums of Understanding/ Agreements with Other Agencies	Improved Collaboration with other Agencies, Stakeholders, and the Private Sector	Developing an Action Plan with Clear Milestones and Metrics	Reporting to Senior Managers on Program Progress and Potential Risks	Taking Actions to Ensure Progress (or Improvements) are Sustained
Initiating or Implementing Legislation and Issuing an Executive Order/ Presidential Initiative	Providing Guidance and Training to Staff and Addressing Skills Gaps	Ensuring there are Processes for Reporting Progress	Tracking Performance Measures and Progress Against Goals	
Issuing Agency Leadership Directives		Making Plans Accessible and Transparent to Other Agencies, Congress, and the Public		
Providing Continuing Oversight and Accountability				

Source: GAO-18-480R | GAO-18-645T

As we reported in the February 2017 high-risk report,[21] the federal government's efforts to address information security deficiencies had fully met one of the five criteria for removal from the High-Risk List—leadership commitment—and partially met the other four, as shown in figure 3. We plan to update our assessment of this high-risk area against the five criteria in February 2019.

Figure 3: Status of High-Risk Area for Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information, as of February 2017
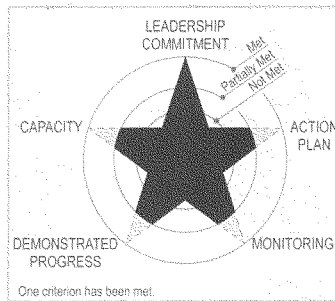
Source: GAO analysis / GAO-18-645T

Note: Each point of the star represents one of the five criteria for removal from the High-Risk List and each ring represents one of the three designations: not met, partially met, or met. An unshaded point at the innermost ring means that the criterion has not been met, a partially shaded point at the middle ring means that the criterion has been partially met, and a fully shaded point at the outermost ring means that the criterion has been met.

[21]GAO-17-317.

Ten Critical Actions Needed to Address Major Cybersecurity Challenges

Based on our prior work, we have identified four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address these challenges, we have identified 10 critical actions that the federal government and other entities need to take (see figure 4). The four challenges and the 10 actions needed to address them are summarized following the table.

20

Figure 4: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges

Major challenges

Critical actions needed

Establishing a comprehensive cybersecurity strategy and performing effective oversight

Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

Address cybersecurity workforce management challenges.

Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

Improve implementation of government-wide cybersecurity initiatives.

Address weaknesses in federal agency information security programs.

Enhance the federal response to cyber incidents.

Protecting cyber critical infrastructure

Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

Improve federal efforts to protect privacy and sensitive data.

Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis. | GAO-18-645T

Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

The federal government has been challenged in establishing a comprehensive cybersecurity strategy and in performing effective oversight as called for by federal law and policy.[22] Specifically, we have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.[23] We have also reported on challenges in performing oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies. The federal government can take four key actions to improve the nation's strategic approach to, and oversight of, cybersecurity.

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.** In February 2013 we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector; however, no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set timeframes for their completion.[24] Accordingly, we recommended that the White House Cybersecurity Coordinator[25] in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a

---

[22]This includes the Federal Information Security Modernization Act of 2014, Revision of the Office of Management and Budget's Circular No. A-130, "*Managing Information as a Strategic Resource*" and Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

[23]GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

[24]GAO-13-187.

[25]In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator to address the recommendations made in the Cyberspace Policy Review, including coordinating interagency cybersecurity policies and strategies and developing a comprehensive national strategy to secure the nation's digital infrastructure.

national strategy[26] including, among other things, milestones and performance measures for major activities to address stated priorities; cost and resources needed to accomplish stated priorities; and specific roles and responsibilities of federal organizations related to the strategy's stated priorities.

In response to our recommendation, in October 2015, the Director of OMB and the Federal Chief Information Officer, issued a *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*.[27] The plan directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The plan also identified key milestones for major activities, resources needed to accomplish milestones, and specific roles and responsibilities of federal organizations related to the strategy's milestones.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. Table 1 identifies these recent efforts and a description of their related contents.

---

[26]In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[27]OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

Table 1: Recent Executive Branch Initiatives That Identify Cybersecurity Priorities for the Federal Government

Executive branch initiative	Date of issuance	Description
Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	May 2017	The Executive Order required federal agencies to take a variety of actions, including to better manage their cybersecurity risks and coordinate to meet reporting requirements related to the cybersecurity of federal networks, critical infrastructure, and the nation.[a] As of July 2018, the executive branch had publicly released several reports, including a high-level assessment by the Office of Management and Budget (OMB) of the cybersecurity risk management capabilities of the federal government.[b] The assessment stated that OMB and the Department of Homeland Security (DHS) examined the capabilities of 96 civilian agencies across 76 cybersecurity metrics and found that 71 agencies had cybersecurity programs that were either at risk or high risk.[c] The report also stated agencies were not equipped to determine how malicious actors seek to gain access to their information systems and data. The report identified core actions to address cybersecurity risks across the federal enterprise.
National Security Strategy	December 2017	The National Security Strategy[d] identified four vital national interests: protecting the homeland, the American people, and American way of life; promoting American prosperity; preserving peace through strength; and advance American influence. The strategy also cites cybersecurity as a national priority and identifies related needed actions, including identifying and prioritizing risk, building defensible government networks, determining and disrupting malicious cyber actors, improving information sharing and deploying layered defenses.
DHS Cybersecurity Strategy	May 2018	The DHS Cybersecurity Strategy[e] articulated seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks. The goals were spread across five pillars that correspond to DHS-wide risk management, including risk identification, vulnerability reduction, threat reduction, consequence mitigation, and enabling cybersecurity outcomes. The strategy is intended to provide DHS with a framework to execute its cybersecurity responsibilities during the next 5 years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

Source: GAO analysis of agency documents | GAO-18-645T

[a]Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order 13800 (Washington, D.C.: May 11, 2017).

[b]OMB, Federal Cybersecurity Risk Determination Report and Action Plan, (Washington, D.C.: May 2018).

[c]OMB and DHS designated agencies as "at risk" if agencies had some essential policies, processes, and tools in place to mitigate overall cybersecurity risks. OMB and DHS designated agencies as "high risk" if agencies did not have essential policies, processes, and tools in place to mitigate overall cybersecurity risks.

[d]The President of the United States, National Security Strategy of the United States of America, (Washington, D.C.: Dec. 2017).

[e]DHS, U.S. Department of Homeland Security Cybersecurity Strategy, (Washington, D.C.: May 2018).

These efforts provide a good foundation toward establishing a more comprehensive strategy, but more effort is needed to address all of the desirable characteristics of a national strategy that we

24

recommended. The recently issued executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. Specifically:

- Milestones and performance measures to gauge results were generally not included in strategy documents. For example, although the DHS Cybersecurity Strategy stated that its implementation would be assessed on an annual basis, it did not describe the milestones and performance measures for tracking the effectiveness of the activities intended to meet the stated goals (e.g., protecting critical infrastructure and responding effectively to cyber incidents). Without such performance measures, DHS will lack a means to ensure that the goals and objectives discussed in the document are accomplished and that responsible parties are held accountable.

  According to officials from DHS's Office of Cybersecurity and Communications, the department is developing a plan for implementing the DHS Cybersecurity Strategy and expects to issue the plan by mid-August 2018. The officials stated that the plan is expected to identify milestones, roles, and responsibilities across DHS to inform the prioritization of future efforts.

- The strategy documents generally did not include information regarding the resources needed to carry out the goals and objectives. For example, although the DHS Cybersecurity Strategy identified a variety of actions the agency planned to take to perform their cybersecurity mission, it did not articulate the resources needed to carry out these actions and requirements. Without information on the specific resources needed, federal agencies may not be positioned to allocate such resources and investments and, therefore, may be hindered in their ability to meet national priorities.

- Most of the strategy documents lacked clearly defined roles and responsibilities for key agencies, such as DHS, DOD, and OMB. These agencies contribute substantially to the nation's cybersecurity programs. For example, although the National Security Strategy discusses multiple priority actions needed to address the nation's cybersecurity challenges (e.g. building defensible government networks and deterring and disrupting malicious cyber actors), it does not describe the roles, responsibilities, or the expected coordination of any specific

federal agencies, including DHS, DOD, or OMB, or other non-federal entities needed to carry out those actions. Without this information, the federal government may not be able to foster effective coordination, particularly where there is overlap in responsibilities, or hold agencies accountable for carrying out planned activities.

Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

- **Mitigate global supply chain risks.** The global, geographically disperse nature of the producers and suppliers of IT products is a growing concern. We have previously reported on potential issues associated with IT supply chain and risks originating from foreign-manufactured equipment. For example, in July 2017, we reported that the Department of State had relied on certain device manufacturers, software developers, and contractor support which had suppliers that were reported to be headquartered in a cyber-threat nation (e.g., China and Russia).[28] We further pointed out that the reliance on complex, global IT supply chains introduces multiple risks to federal agencies, including insertion of counterfeits, tampering, or installation of malicious software or hardware.

  Earlier this month, we testified that if such global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.[29] Thus, the potential exists for serious adverse impact on an agency's operations, assets, and employees. These factors highlight the importance and urgency of federal agencies appropriately assessing, managing, and monitoring IT supply chain risk as part of their agencywide information security programs.

- **Address cybersecurity workforce management challenges.** The federal government faces challenges in ensuring that the nation's cybersecurity workforce has the appropriate skills. For example, in June 2018, we reported on federal efforts to implement the

---

[28]GAO, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, GAO-17-688R (Washington, D.C.: July 27, 2017).

[29]GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (Washington, D.C.: July 12, 2018).

requirements of the *Federal Cybersecurity Workforce Assessment Act of 2015.*[30] We determined that most of the Chief Financial Officers (CFO) Act[31] agencies had not fully implemented all statutory requirements, such as developing procedures for assigning codes to cybersecurity positions. Further, we have previously reported that DHS and DOD had not addressed cybersecurity workforce management requirements set forth in federal laws.[32] In addition, we have reported in the last 2 years that federal agencies (1) had not identified and closed cybersecurity skills gaps,[33] (2) had been challenged with recruiting and retaining qualified staff,[34] and (3) had difficulty navigating the federal hiring process.[35]

A recent executive branch report also discussed challenges associated with the cybersecurity workforce. Specifically, in response to Executive Order 13800, the Department of Commerce and DHS led an interagency working group exploring how to support the growth and sustainment of future cybersecurity employees in the public and

---

[30]GAO, *Cybersecurity Workforce: Agencies Need to improve Baseline Assessments and Procedures for Coding positions*, GAO-18-466 (Washington, D.C.: June 14, 2018). The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted as part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (Dec. 18, 2015).

[31]There are 24 agencies identified in the Chief Financial Officers Act: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[32]GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018); and *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements*, GAO-18-47 (Washington, D.C.: Nov. 30, 2017).

[33]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[34]GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

[35]GAO, *Federal Hiring: OPM Needs to Improve Management and Oversight of Hiring Authorities*, GAO-16-521 (Washington, D.C.: Aug. 2, 2016).

private sectors. In May 2018, the departments issued a report[36] that identified key findings, including:

- the U.S. cybersecurity workforce needs immediate and sustained improvements;

- the pool of cybersecurity candidates needs to be expanded through retraining and by increasing the participation of women, minorities, and veterans;

- a shortage exists of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors; and

- comprehensive and reliable data about cybersecurity workforce position needs and education and training programs are lacking.

The report also included recommendations and proposed actions to address the findings, including that private and public sectors should (1) align education and training with employers' cybersecurity workforce needs by applying the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework; (2) develop cybersecurity career model paths; and (3) establish a clearinghouse of information on cybersecurity workforce development education, training, and workforce development programs and initiatives.

In addition, in June 2018, the executive branch issued a government reform plan and reorganization recommendations that included, among other things, proposals for solving the federal cybersecurity workforce shortage.[37] In particular, the plan notes that the administration intends to prioritize and accelerate ongoing efforts to reform the way that the federal government recruits, evaluates, selects, pays, and places cyber talent across the enterprise. The plan further states that, by the end of the first quarter of fiscal year 2019, all CFO Act agencies, in coordination with DHS and OMB, are to develop a critical list of vacancies across their organizations. Subsequently, OMB and DHS are to analyze these lists and work with OPM to

---

[36]The Secretaries of Commerce and Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*, (Washington, D.C.: May 2018).

[37]Executive Office of the President of the United States, *Delivering Government Solutions in the 21st Century: Reform Plan and Reorganization Recommendations* (Washington, D.C.: June 2018).

develop a government-wide approach to identifying or recruiting new employees or reskilling existing employees. Regarding cybersecurity training, the plan notes that OMB is to consult with DHS to standardize training for cybersecurity employees, and should work to develop an enterprise-wide training process for government cybersecurity employees.

- **Ensure the security of emerging technologies.** As the devices used in daily life become increasingly integrated with technology, the risk to sensitive data and PII also grows. Over the last several years, we have reported on weaknesses in addressing vulnerabilities associated with emerging technologies, including:

  - IoT devices, such as fitness trackers, cameras, and thermostats, that continuously collect and process information are potentially vulnerable to cyber-attacks;[38]

  - IoT devices, such as those acquired and used by DOD employees or that DOD itself acquires (e.g., smartphones), may increase the security risks to the department;[39]

  - vehicles that are potentially susceptible to cyber-attack through technology, such as Bluetooth;[40]

  - the unknown impact of artificial intelligence cybersecurity; and[41]

  - advances in cryptocurrencies and blockchain technologies.[42]

Executive branch agencies have also highlighted the challenges associated with ensuring the security of emerging technologies. Specifically, in a May 2018 report issued in response to Executive Order 13800, the Department of Commerce and DHS issued a report

---

[38]GAO, *Technology Assessment: Internet of Things: Status and Implications of an Increasingly Connected World*, GAO-17-75 (Washington, D.C.: May 15, 2017).

[39]GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

[40]GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Apr. 25, 2016).

[41]GAO, *Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 28, 2018).

[42]GAO, *GAO Strategic Plan 2018-2023: Trends Affecting Government and Society*, GAO-18-396SP (Washington, D.C.: Feb. 22, 2018).

on the opportunities and challenges in reducing the botnet threat.[43] The opportunities and challenges are centered on six principal themes, including the global nature of automated, distributed attacks; effective tools; and awareness and education. The report also provides recommended actions, including that federal agencies should increase their understanding of what software components have been incorporated into acquired products and establish a public campaign to support awareness of IoT security.

In our previously discussed reports related to this cybersecurity challenge, we made a total of 50 recommendations to federal agencies to address the weaknesses identified. As of July 2018, 48 recommendations had not been implemented. These outstanding recommendations include 8 priority recommendations, meaning that we believe that they warrant priority attention from heads of key departments and agencies. These priority recommendations include addressing weaknesses associated with, among other things, agency-specific cybersecurity workforce challenges and agency responsibilities for supporting mitigation of vehicle network attacks. Until our recommendations are fully implemented, federal agencies may be limited in their ability to provide effective oversight of critical government-wide initiatives, address challenges with cybersecurity workforce management, and better ensure the security of emerging technologies.

In addition to our prior work related to the federal government's efforts to establish key strategy documents and implement effective oversight, we also have several ongoing reviews related to this challenge. These include reviews of:

- the CFO Act agencies' efforts to submit complete and reliable baseline assessment reports of their cybersecurity workforces;

- the extent to which DOD has established training standards for cyber mission force personnel, and efforts the department has made to achieve its goal of a trained cyber mission force;

- selected agencies' ability to implement cloud service technologies and notable benefits this might have on agencies; and

---

[43]The Secretaries of Commerce and Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, (Washington, D.C.: May 22, 2018).

- the federal approach and strategy to securing agency information systems, to include federal intrusion detection and prevention capabilities and the intrusion assessment plan.

Securing Federal Systems and Information

The federal government has been challenged in securing federal systems and information. Specifically, we have reported that federal agencies have experienced challenges in implementing government-wide cybersecurity initiatives, addressing weaknesses in their information systems and responding to cyber incidents on their systems. This is particularly concerning given that the emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. As such, it is important that federal agencies take appropriate steps to better ensure they have effectively implemented programs to protect their information and systems. We have identified three actions that the agencies can take.

- **Improve implementation of government-wide cybersecurity initiatives.** Specifically, in January 2016, we reported that DHS had not ensured that the National Cybersecurity Protection System (NCPS) had fully satisfied all intended system objectives related to intrusion detection and prevention, information sharing, and analytics.[44] In addition, in February 2017, we reported[45] that the DHS National Cybersecurity and Communications Integration Center's (NCCIC)[46] functions were not being performed in adherence with the

---

[44]GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016). NCPS is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

[45]GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

[46]DHS established the NCCIC as to serve as the 24/7 cyber monitoring, incident response, and management center. The center provides a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats.

principles set forth in federal laws.[47] We noted that, although NCCIC was sharing information about cyber threats in the way it should, the center did not have metrics to measure that the information was timely, relevant and actionable, as prescribed by law.

- **Address weaknesses in federal information security programs.** We have previously identified a number of weaknesses in agencies' protection of their information and information systems. For example, over the past 2 years, we have reported that:

  - most of the 24 agencies covered by the CFO Act had weaknesses in each of the five major categories of information system controls (i.e., access controls, configuration management controls, segregation of duties, contingency planning, and agency-wide security management);[48]

  - three agencies—the Securities Exchange Commission, the Federal Deposit Insurance Corporation, and the Food and Drug Administration—had not effectively implemented aspects of their information security programs, which resulted in weaknesses in these agencies' security controls;[49]

  - information security weaknesses in selected high-impact systems at four agencies—the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, OPM, and the Department of Veterans Affairs—were cited as a key reason that the agencies had not effectively implemented elements of their information security programs;[50]

---

[47] *The National Cybersecurity Protection Act of 2014* and *Cybersecurity Act of 2015* require NCCIC to carry out 11 cybersecurity functions, to the extent practicable, in accordance with nine principles. Pub. L. No. 113-282, Dec. 18, 2014. The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

[48] GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

[49] GAO, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions*, GAO-17-469 (Washington, D.C.: July 27, 2017); *Information Security: FDIC Needs to Improve Controls over Financial Systems and Information*, GAO-17-436 (Washington, D.C.: May 31, 2017); and *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk*, GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

[50] GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

- DOD's process for monitoring the implementation of cybersecurity guidance had weaknesses and resulted in the closure of certain tasks (such as completing cyber risk assessments) before they were fully implemented;[51] and

- agencies had not fully defined the role of their Chief Information Security Officers, as required by FISMA.[52]

We also recently testified that, although the government had acted to protect federal information systems, additional work was needed to improve agency security programs and cyber capabilities. [53]In particular, we noted that further efforts were needed by agencies to implement our prior recommendations in order to strengthen their information security programs and technical controls over their computer networks and systems.

- **Enhance the federal response to cyber incidents.** We have reported that certain agencies have had weaknesses in responding to cyber incidents. For example,

  - as of August 2017, OPM had not fully implemented controls to address deficiencies identified as a result of its 2015 cyber incidents;[54]

  - DOD had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises.[55]

  - as of April 2016, DOD had not identified, clarified, or implemented all components of its support of civil authorities during cyber incidents;[56] and

---

[51]GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened*, GAO-17-512 (Washington, D.C.: Aug. 1, 2017).

[52]GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

[53]GAO, *Information Technology: Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity*, GAO-18-566T (Washington, D.C.: May 23, 2018).

[54]GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[55]GAO, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises*, GAO-16-574 (Washington, D.C.: Sept. 6, 2016).

- as of January 2016, DHS's NCPS had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.[57]

In the public versions of the reports previously discussed for this challenge area, we made a total of 101 recommendations to federal agencies to address the weaknesses identified.[58] As of July 2018, 61 recommendations had not been implemented. These outstanding recommendations include 14 priority recommendations to address weaknesses associated with, among other things, the information security programs at the National Aeronautics and Space Administration, OPM, and the Security Exchange Commission. Until these recommendations are implemented, these federal agencies will be limited in their ability to ensure the effectiveness of their programs for protecting information and systems.

In addition to our prior work, we also have several ongoing reviews related to the federal government's efforts to protect its information and systems. These include reviews of:

- Federal Risk and Authorization Management Program (FedRAMP)[59] implementation, including an assessment of the implementation of the program's authorization process for protecting federal data in cloud environments;

- the Equifax data breach, including an assessment of federal oversight of credit reporting agencies' collection, use, and protection of consumer PII;

---

[56]GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, D.C.: Apr. 4, 2016).

[57]GAO-16-294.

[58]GAO often issues two versions of its audit reports on the security of federal systems and information. One version is publicly available, and one version is not available to the public because of the sensitive security information it contains. GAO has made hundreds of recommendations to agencies to rectify technical security control deficiencies identified in these non-publicly available reports.

[59]In December 2011, OMB established FEDRAMP—a government-wide program intended to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud computing products and services.

- the Federal Communication Commission's Electronic Comment Filing System security, to include a review of the agency's detection of and response to a May 2017 incident that reportedly impacted the system;

- DOD's efforts to improve the cybersecurity of its major weapon systems;

- DOD's whistleblower program, including an assessment of the policies, procedures, and controls related to the access and storage of sensitive and classified information needed for the program;

- IRS's efforts to (1) implement security controls and the agency's information security program, (2) authenticate taxpayers, and (3) secure tax information; and

- federal intrusion detection and prevention capabilities.

Protecting Cyber Critical Infrastructure

The federal government has been challenged in working with the private sector to protect critical infrastructure. This infrastructure includes both public and private systems vital to national security and other efforts, such as providing the essential services that underpin American society. As the cybersecurity threat to these systems continues to grow, federal agencies have millions of sensitive records that must be protected. Specifically, this critical infrastructure threat could have national security implications and more efforts should be made to ensure that it is not breached.

To help address this issue, NIST developed the cybersecurity framework—a voluntary set of cybersecurity standards and procedures for industry to adopt as a means of taking a risk-based approach to managing cybersecurity.[60]

However, additional action is needed to strengthen the federal role in protecting the critical infrastructure. Specifically, we have reported on other critical infrastructure protection issues that need to be addressed. For example:

- Entities within the 16 critical infrastructure sectors reported encountering four challenges to adopting the cybersecurity framework, such as being limited in their ability to commit necessary

---

[60] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). The cybersecurity framework was updated on April 16, 2018.

resources towards framework adoption and not having the necessary knowledge and skills to effectively implement the framework.[61]

- Major challenges existed to securing the electricity grid against cyber threats.[62] These challenges included monitoring implementation of cybersecurity standards, ensuring security features are built into smart grid systems, and establishing metrics for cybersecurity.

- DHS and other agencies needed to enhance cybersecurity in the maritime environment. Specifically, DHS did not include cyber risks in its risk assessments that were already in place nor did it address cyber risks in guidance for port security plans.[63]

- Sector-specific agencies[64] were not properly addressing progress or metrics to measure their progress in cybersecurity.[65]

- DOD and the Federal Aviation Administration identified a variety of operations and physical security risks that could adversely affect DOD missions.[66]

We made a total of 19 recommendations to federal agencies to address these weaknesses and others. These recommendations include, for example, a total of 9 recommendations to 9 sector-specific agencies to develop methods to determine the level and type of cybersecurity framework adoption across their respective sectors.[67] As of July 2018, all

---

[61]GAO, *Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

[62]GAO, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention*, GAO-16-174T (Washington, D.C.: Oct. 21, 2015).

[63]GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity*, GAO-16-116T (Washington, D.C.: Oct. 8, 2015).

[64]Sector-specific agencies are federal departments or agencies with responsibility for providing institutional knowledge and specialized expertise. They accomplish this by leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the environment.

[65]GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015). The government facilities sector was excluded from the scope of this review due to its uniquely governmental focus.

[66]GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft*, GAO-18-177 (Washington, D.C.: Jan. 18, 2018).

[67]GAO-18-211.

19 recommendations had not been implemented. Until these recommendations are implemented, the federal government will continue to be challenged in fulfilling its role in protecting the nation's critical infrastructure.

In addition to our prior work related to the federal government's efforts to protect critical infrastructure, we also have several ongoing reviews focusing on:

- the physical and cybersecurity risks to pipelines across the country responsible for transmitting oil, natural gas, and other hazardous liquids;
- the cybersecurity risks to the electric grid; and
- the privatization of utilities at DOD installations.

Protecting Privacy and Sensitive Data

The federal government has been challenged in protecting privacy and sensitive data. Advances in technology, including powerful search technology and data analytics software, have made it easy to correlate information about individuals across large and numerous databases, which have become very inexpensive to maintain. In addition, ubiquitous Internet connectivity has facilitated sophisticated tracking of individuals and their activities through mobile devices such as smartphones and fitness trackers.

Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of PII maintained by government agencies or on their behalf are protected both from inappropriate access (i.e., data breaches) as well as inappropriate use (i.e., for purposes not originally specified when the information was collected). Likewise, the trend in the private sector of collecting extensive and detailed information about individuals needs appropriate limits. The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.

Federal agencies should take two types of actions to address this challenge area. In addition, we have previously proposed two matters for congressional consideration aimed toward better protecting PII.

- **Improve federal efforts to protect privacy and sensitive data.** We have issued several reports noting that agencies had deficiencies in

protecting privacy and sensitive data that needed to be addressed. For example:

- The Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS) and external entities were at risk of compromising Medicare Beneficiary Data due to a lack of guidance and proper oversight.[68]

- The Department of Education's Office of Federal Student Aid had not properly overseen its school partners' records or information security programs.[69]

- HHS had not fully addressed key security elements in its guidance for protecting the security and privacy of electronic health information.[70]

- CMS had not fully protected the privacy of users' data on state-based marketplaces.[71]

- Poor planning and ineffective monitoring had resulted in the unsuccessful implementation of government initiatives aimed at eliminating the unnecessary collection, use, and display of SSNs.[72]

- **Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.** We have issued a series of reports that highlight a number of the key concerns in this area. For example:

- The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent;[73]

---

[68]GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*, GAO-18-210 (Washington, D.C.: Mar. 6, 2018).

[69]GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information*, GAO-18-121 (Washington, D.C.: Dec. 15, 2017).

[70]GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

[71]GAO, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls*, GAO-16-265 (Washington, D.C.: Mar. 23, 2016).

[72]GAO, *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display*, GAO-17-553 (Washington, D.C.: July 25, 2017).

[73]GAO-17-75.

- Federal laws for smartphone tracking applications have not generally been well enforced.[74]

- The FBI has not fully ensured privacy and accuracy related to the use of face recognition technology.[75]

We have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974[76] and the E-Government Act of 2002,[77] because they may not consistently protect PII.[78] Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect PII in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. However, revisions to the Privacy Act and the E-Government Act have not yet been enacted.

Further, we also suggested that Congress consider strengthening the consumer privacy framework[79] and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices.[80] However, these suggested changes have not yet been enacted.

We also made a total of 29 recommendations to federal agencies to address the weaknesses identified. As of July 2018, 28 recommendations had not been implemented. These outstanding recommendations include 6 priority recommendations to address weaknesses associated with,

[74]GAO, *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking*, GAO-16-317 (Washington, D.C.: Apr. 21, 2016).

[75]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[76]Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

[77]Pub. L. No. 107-347, 116 Stat. 2899.

[78]GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

[79]This framework presents a consumer privacy bill of rights, describes a stakeholder process to specify how the principles in that bill of rights would apply, and encourages Congress to provide the Federal Trade Commission with enforcement authorities for the bill of rights.

[80]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

among other things, publishing privacy impact assessments[81] and improving the accuracy of the FBI's face recognition services. Until these recommendations are implemented, federal agencies will be challenged in their ability to protect privacy and sensitive data and ensure that its collection and use is appropriately limited.

In addition to our prior work, we have several ongoing reviews related to protecting privacy and sensitive data. These include reviews of:

- IRS's taxpayer authentication efforts, including what steps the agency is taking to monitor and improve its authentication methods;
- the extent to which the Department of Education's Office of Federal Student Aid's policies and procedures for overseeing non-school partners' protection of federal student aid data align with federal requirements and guidance;
- data security issues related to credit reporting agencies, including a review of the causes and impacts of the August 2017 Equifax data breach;
- the extent to which Equifax assessed, responded to, and recovered from its August 2017 data breach;
- federal agencies' efforts to remove PII from shared cyber threat indicators; and
- how the federal government has overseen Internet privacy, including the roles of the Federal Communications Commission and the Federal Trade Commission, and strengths and weaknesses of the current oversight authorities.

In summary, since 2010, we have made over 3,000 recommendations to agencies aimed at addressing the four cybersecurity challenges. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. Of the roughly 3,000 recommendations made since 2010, nearly 1,000 had not been implemented as of July 2018. We have also designated 35 as priority recommendations, and as of July 2018, 31 had not been implemented.

---

[81]Privacy impact assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system.

The federal government and the nation's critical infrastructure are dependent on IT systems and electronic data, which make them highly vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's security, prosperity, and well-being. Nevertheless, the security over these systems and data is inconsistent and urgent actions are needed to address ongoing cybersecurity and privacy challenges. Specifically, the federal government needs to implement a more comprehensive cybersecurity strategy and improve its oversight, including maintaining a qualified cybersecurity workforce; address security weaknesses in federal systems and information and enhance cyber incident response efforts; bolster the protection of cyber critical infrastructure; and prioritize efforts to protect individual's privacy and PII. Until our recommendations are addressed and actions are taken to address the four challenges we identified, the federal government, the national critical infrastructure, and the personal information of U.S. citizens will be increasingly susceptible to the multitude of cyber-related threats that exist.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contacts and Staff Acknowledgments

Questions about this testimony can be directed to Nick Marinos, Director, Cybersecurity and Data Protection Issues, at (202) 512-9342 or marinosn@gao.gov; and Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jon Ticehurst, Assistant Director; Kush K. Malhotra, Analyst-In-Charge; Chris Businsky; Alan Daigle; Rebecca Eyler; Chaz Hubbard; David Plocher; Bradley Roach; Sukhjoot Singh; Di'Mond Spencer; and Umesh Thakkar.

Related GAO Reports

Information Security: Supply Chain Risks Affecting Federal Agencies. GAO-18-667T. Washington, D.C.: July 12, 2018.

Information Technology: Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity. GAO-18-566T. Washington, D.C.: May 23, 2018.

Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement. GAO-18-210. Washington, D.C.: April 5, 2018.

Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications. GAO-18-142SP. Washington, D.C.: March 28, 2018.

GAO Strategic Plan 2018-2023: Trends Affecting Government and Society. GAO-18-396SP. Washington, D.C.: February 22, 2018.

Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption. GAO-18-211. Washington, D.C.: February 15, 2018.

Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements. GAO-18-175. Washington, D.C.: February 6, 2018.

Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft. GAO-18-177. Washington, D.C.: January 18, 2018.

Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information. GAO-18-121. Washington, D.C.: December 15, 2017.

Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements. GAO-18-47. Washington, D.C.: November 30, 2017.

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices. GAO-17-549. Washington, D.C.: September 28, 2017.

Information Security: OPM Has Improved Controls, but Further Efforts Are Needed. GAO-17-614. Washington, D.C.: August 3, 2017.

42

Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened. GAO-17-512. Washington, D.C.: August 1, 2017.

State Department Telecommunications: Information on Vendors and Cyber-Threat Nations. GAO-17-688R. Washington, D.C.: July 27, 2017.

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD. GAO-17-668. Washington, D.C.: July 27, 2017.

Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions. GAO-17-469. Washington, D.C.: July 27, 2017.

Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data. GAO-17-395. Washington, D.C.: July 26, 2017.

Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display. GAO-17-553. Washington, D.C.: July 25, 2017.

Information Security: FDIC Needs to Improve Controls over Financial Systems and Information. GAO-17-436. Washington, D.C.: May 31, 2017.

Technology Assessment: Internet of Things: Status and Implications of an Increasingly Connected World. GAO-17-75. Washington, D.C.: May 15, 2017.

Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely. GAO-17-163. Washington, D.C.: February 1, 2017.

High-Risk Series: An Update. GAO-17-317. Washington, D.C.: February 2017.

IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps. GAO-17-8. Washington, D.C.: November 30, 2016.

43

Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight. GAO-16-771. Washington, D.C.: September 26, 2016.

Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises. GAO-16-574. Washington, D.C.: September 6, 2016.

Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk. GAO-16-513. Washington, D.C.: August 30, 2016.

Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority. GAO-16-686. Washington, D.C.: August 26, 2016.

Federal Hiring: OPM Needs to Improve Management and Oversight of Hiring Authorities. GAO-16-521. Washington, D.C.: August 2, 2016.

Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems. GAO-16-501. Washington, D.C.: May 18, 2016.

Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy. GAO-16-267. Washington, D.C.: May 16, 2016.

Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking. GAO-16-317. Washington, D.C.: May 9, 2016.

Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack. GAO-16-350. Washington, D.C.: April 25, 2016.

Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents. GAO-16-332. Washington, D.C.: April 4, 2016.

Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls. GAO-16-265. Washington, D.C.: March 23, 2016.

Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System. GAO-16-294. Washington, D.C.: January 28, 2016.

44

Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress. GAO-16-79. Washington, D.C.: November 19, 2015.

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention. GAO-16-174T. Washington, D.C.: October 21, 2015.

Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity. GAO-16-116T. Washington, D.C.: October 8, 2015.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. Washington, D.C.: February 14, 2014.

Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace. GAO-13-663. Washington, D.C.: September 25, 2013.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information. GAO-08-536. Washington, D.C.: May 19, 2008.

Mr. HURD. Thank you, Mr. Dodaro.

Ms. Kent, you're now recognized for 5 minutes for opening remarks.

STATEMENT OF SUZETTE KENT

Ms. KENT. Chairman Hurd, Chairman Meadows, Ranking Member Kelly, Ranking Member Connolly, and members of the committee, thank you for having me here today. I am honored to be here to speak with you, and I appreciate all the forums that inspire more aggressive actions towards improving Federal cybersecurity.

My goal today is to share with you the progress that has been made against the areas highlighted by the comptroller general, but more important, to share the perspectives on what still needs to be done. And I'd like to engage your continued support on that.

Advancement of our cybersecurity posture, both at agency levels and across the Federal enterprise, is one of the most important parts of my job. Tomorrow will actually mark 5 months serving at OMB as the Federal chief information officer. And I joined from the financial services industry where the bar is high for cybersecurity and data protection, and I bring that same high bar of expectations to my role as Federal CIO.

I was fortunate to come into the role when the administration was setting out the President's Management Agenda that focuses on technology modernization, data accountability and transparency, and building the workforce of the 21st century.

Cybersecurity is a core component of the PMA's IT modernization goals. It's also embedded in the work that we are driving under other goals. The goals for sharing quality services and improving IT spending have elements that drive the use of modern technologies and industry best practices to improve our overall cyber posture.

Additionally, the PMA stresses strategies for recruiting, retaining, and re-skilling our Federal IT and cybersecurity workforce, because our current status is as much a people issue as it is a technology issue. While the PMA outlines the critical areas of focus, OMB's statutory cybersecurity roles are predominately defined by the E–Government Act of 2002 and the Federal Information Security Modernization Act of 2014.

Our roles align to three main things: development of policy and oversight for the Federal civilian systems, Assisting agencies with data analysis and budget, and gathering evidence that promotes solutions that achieve these policies and standards. To carry out the responsibilities, we work closely with agency technology leaders, DHS, NIST, DOD, the intelligence community, and the National Security Council.

But because cybersecurity requires deep expertise both about technology and the mission functions, it does take a collaborative approach to address both the agency-specific and enterprise demands. I am united with the Federal Inspector General community in the mission of securing our systems and data on a journey that actually doesn't end.

The improvements in Federal cybersecurity outlined in GAO's report are due to a focus on accountability, and it's my goal to further

advance the culture of continuous evolution of our cyber capabilities and our workforce to tackle the things that we still must do.

In May of 2017, the President signed Executive Order 13800 regarding strengthening cybersecurity of Federal networks. This executive order recognized that we need to defend the security of citizen information and ensure the agencies consider cybersecurity as a vital part of their core mission. As part of this EO, the White House also published a report to the President on Federal IT modernization, which included 52 tasks, such as safeguarding high-value assets, network consolidation, use of commercial cloud solutions, and strengthening identity management tactics. I share with you today that 37 of those 52 tasks have been completed, many of them ahead of schedule, and we intend to complete the remaining tasks by the end of the year.

Executive Order 13800 also directed OMB to develop the Federal Cybersecurity Risk Determination Report and an action plan. Together, OMB and DHS conducted agency risk management assessments to measure agency cybersecurity capabilities, and very specifically, their risk mitigation approaches. This report did evidence that there's still much to do to improve the awareness of the threat environment, and we're using these finding to prioritize both the investments and the focus of resources.

There are other key initiatives I'll quickly highlight. As chair of the Technology Modernization Board, I'm excited by the way this vehicle supports acceleration of modernization, and we appreciate the funding that Congress provided this year, and we hope to receive funding for next year. We are focused on enhancing CIO authorities.

And, lastly, and most importantly, we are updating old policies, policies that are not effective given the current state of technology capabilities. We're delivering new policies for high-value assets, data centers, continuous monitoring cloud technologies, and network optimization in the next coming months.

In closing, I'm fortunate to take on this role with a clear and focused technology agenda. Cybersecurity has to underpin everything we're doing, from acquisition to operations, because the battle is continuous and our effort to raise the bar and outpace our adversaries is a mission imperative for every agency.

I look forward to working with Congress and the leaders across the Federal Government agencies to be aggressive and relentless about approving Federal cybersecurity. And I thank you for the opportunity to talk with you today.

[Prepared statement of Ms. Kent follows:]

Testimony to House Committee on Oversight and Government Reform

Suzette Kent

Federal Chief Information Officer

Office of Management and Budget

July 25, 2018

Government Accountability Office's High Risk Cybersecurity Issues Report

Chairman Hurd, Chairman Meadows, Ranking Member Kelly, Ranking Member Connolly and Members of the Committees, thank you for having me here today.

Tomorrow will mark five months serving as the Federal Chief Information Officer (Federal CIO) within the Office of Management and Budget (OMB). In the short time in my role, I have had the great opportunity to learn from and work with a tremendous number of talented, driven, thoughtful, and passionate technology and cybersecurity professionals across the Federal Government. I am honored to be here today to talk with you and I appreciate participating in forums that draw attention and inspire actions toward improving federal cyber security. Advancement of our cyber security posture both at Agency level and across the government enterprise is one of the most important parts of my job.

My goal in being here today is to share with you some of the progress that has been made against the areas highlighted by GAO, but also to share what still must be done and engage your continued support against these objectives. I joined the Federal Government five months ago tomorrow from the Financial Services

industry where cybersecurity and data protection are at the core of industry capabilities. I bring that high bar of expectation to my role as Federal CIO.

As the Federal CIO, I am responsible for assisting Director Mulvaney in implementing OMB's statutory role per the E-Government Act of 2002 and the Federal Information Security Modernization Act of 2014 (FISMA).[1] These statutory roles include improving the management and operations of Federal civilian information technology systems and overseeing the information security programs of non-National Security Systems. It is important to note that the FISMA cybersecurity responsibilities for National Security Systems is delegated to the Director of National Intelligence and the Secretary of Defense. For those non-National Security Systems, the Office of the Federal CIO (OFCIO), executes OMB's statutory roles by developing and overseeing the implementation of policies and guidelines. OFCIO works with Federal civilian agency leadership to address information security priorities, collaborates with partners to develop cybersecurity policies, and conducts data-driven oversight of agency cybersecurity programs.

OMB's cybersecurity responsibilities under FISMA are addressed by three areas we focus on:

1. Developing and overseeing the implementation of cybersecurity policies and guidance for Federal civilian information technology systems.
2. Collaborating with agencies to protect federal civilian information technology systems and establishing a risk based approach to cybersecurity.
3. Ensuring that agencies are complying with federal cybersecurity policies and standards, in coordination with the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS).

In addition to these specific responsibilities, OMB works closely with our partners across government to ensure the security of the Federal civilian enterprise. This includes working with DHS, the National Security Council (NSC), Intelligence Community, Department of Defense (DoD), and others to respond to significant cybersecurity incidents and breaches. We also coordinate with agency Chief

---

[1] Public Law (P.L.) 113-283, FISMA Modernization Act of 2014 (2014), https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

Information Officers (CIOs) and Chief Information Security Officers (CISOs) to improve their ability to allocate resources to manage cyber risks within their department or agency. Improving communication, coordination, and implementation of the various roles and responsibilities set forth under FISMA is a critical task, and one I take very seriously as the Federal CIO, but it is only a part of this Administration's larger cybersecurity efforts.

We also collaborate with the Federal Inspectors General (IG) community to drive accountability and improve cybersecurity program performance across the government. We work closely with the IGs, CIOs, and CISOs. Throughout our collaboration, we work toward the same mission of securing Federal information and information systems. The improvements in Federal cybersecurity over the past few years, which GAO outlines in its most recent High Risk report, are a due to a culture of accountability and performance that we have enhanced with our oversight partners.

This Administration has made it a priority to improve our nation's cybersecurity. In May 2017, the President signed Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (EO 13800)[2] to enhance cybersecurity risk management across the Federal Government. This executive order recognizes that the Government must promote the security of citizens' information and ensure that agencies consider cybersecurity as a vital element of their core missions and services, including the fundamental threat to mission and services posed by malicious cyber actors. The Executive Order also directed OMB, DoD, DHS, and the Director of National Intelligence, among other agencies to assess risks within their respective purviews, and develop action plans and strategies to mitigate those risks.

Pursuant to EO 13800, the White House published the Report to the President on Federal IT Modernization[3] (IT Modernization Report) in December 2017. In addition to surveying the state of Federal IT, the IT Modernization Report included 52 discreet, time-bound tasks focused on modernizing and safeguarding

---

[2] White House, Executive Order 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[3] American Technology Council, Report to the President on Federal IT Modernization (2017), https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Moderni zation%20-%20Final.pdf.

High Value Assets (HVAs), promoting the consolidation of network acquisitions and management, and driving agencies to leverage commercial cloud solutions and cybersecurity shared services. OMB, in coordination with DHS, NIST, and the General Services Administration (GSA), has completed 37 of those 52 tasks, many ahead of schedule. We intend to complete the rest of the tasks on time and by the end of the year.

In addition to the IT Modernization Report, EO 13800 required OMB to develop the *Federal Cybersecurity Risk Determination Report and Action Plan*, which provides a comprehensive review of Federal agencies' cybersecurity programs to date. OMB and DHS conducted 97 agency risk management assessments to measure the sufficiency of agencies' cybersecurity capabilities and risk mitigation approaches. OMB found that agencies lack situational awareness of the threat environment, capabilities to detect intrusions and data exfiltration, and fundamental accountability for mitigating cyber risks across the enterprise. OMB is leveraging these findings to drive returns on investment across the $15 billion in Federal cybersecurity spending in terms of reducing risks to the Federal enterprise.

We are currently working on many other initiatives to drive stronger accountability and improvement in Federal cybersecurity. As the Chair of the Technology Modernization Board, I am working to administer the Technology Modernization Fund to drive high impact investments to reduce or upgrade outdated legacy systems and improve agency service delivery. We appreciate the $100 million investment by Congress in FY 2018 for this important initiative and we look forward to working with this Committee and the Appropriations Committees to secure more funding in FY 2019 to continue our modernization efforts and multiply the impact and scope of the projects the TMF can fund.

We are working with the White House and Federal agencies to implement Executive Order 13833, which clarifies and reinforces the authorities and provenance of agency CIOs in IT budgeting and making risk based determinations across agency IT investments. We are working with the Federal community to better understand agency issues and incorporate that into OMB guidance. We are expecting to deliver new, updated, iterative policies around securing high value assets, data center optimization, information security continuous monitoring, and

network optimization and performance in the coming months. These policies will allow the Federal government to make smarter, risk informed investment and leverage modern technologies and enable our agencies to be more agile, responsive, and secure – which are goals OMB, GAO, and Congress all share.

Cybersecurity is a core component of the President's Management Agenda (PMA). IT Modernization goals, but it is also embedded in the work we are driving under the Sharing Quality Services Goal, the Improving IT Spending Goal, and many other subgoals and strategies anchored throughout the entire PMA. Further, both the PMA and the recent Reshaping American Government in the 21st Century reorganization and reform plan include explicit strategies and milestones to retain, reskill, and modernize our Federal IT and cybersecurity workforce, because security is as much a personnel issue as it is a technology issue.

The Deputy Secretaries and other senior officials who make up the President's Management Council, as well as OFCIO, DHS, and additional agency leadership are committed to continuous improvement and excellence in these areas.

These success stories underscore the great work that has occurred and illustrate the work that remains before us. It is also critical to showcase the success stories across agencies and outside government to prove that we can be successful and share the path to success so that Agency teams can leverage the experiences of others and have the confidence of achievable goals. By successfully delivering on our agenda, we build trust with the American public, and our stakeholders in Congress and the Administration. In this regard, I was fortunate to take on my current role with a clear, focused agenda against which we can execute. My job is to build relationships, eliminate blockers, and focus time, money, and attention – where warranted and effective – to propel further success in these vital cybersecurity areas.

Cybersecurity must underpin everything we are doing with respect to acquiring, deploying, operating and maintaining information technology across the government. The threats to our Nation continues to increase as our systems become more interconnected and malicious tools become more available. We are working across Federal agencies and industry to drive a risk management culture and reduce the impact that cyber incidents can have on core government

functions. I look forward to working with Comptroller General Dodaro and GAO, and our other Federal partners to enhance the government's security posture.

Thank you again for inviting me here today. I look forward to answering your questions.

Mr. HURD. Thank you, Ms. Kent.

Now we'll go to the first round of questions. The distinguished gentleman from Georgia is now recognized for 5 minutes.

Mr. HICE. Thank you very much, Mr. Chairman. Thank you both for being here. Mr. Dodaro, good seeing you again. And, Ms. Kent, congratulations on your recent position.

Last year, fiscal year 2017, Federal civilian agencies reported over 35,000 information security incidents. That's a stunning number, about a 15 percent increase from the previous year.

This is really to both of you to begin with. What's driving that increase?

Mr. DODARO. I think there's at least two things. One, there's a better awareness on the part of the agencies to report incidents, which do occur. But I also think that it's being driven in part by more aggressive activity on the part of state and non-state actors to try to penetrate the Federal Government systems. This applies to critical infrastructure protection as well. And so I think it's, you know, both—both factors are at play here at a minimum.

Ms. KENT. I concur. And we do see an increase across the entire industry in threats, but you also see the increase in reporting, and that's something that we need to continue to move more aggressively across all of the agencies.

Mr. HICE. All right. So it's both, and we're having more incidents, more attacks, and we're also getting better at detecting them?

Ms. KENT. Yes.

Mr. HICE. All right. Can you walk me through some of the various means that attackers use to initiate some sort of cyber attack, the threat vectors? What's most common? What's most preventable?

Mr. Dodaro.

Mr. DODARO. Yeah. There's—you know, phishing attacks have been particularly prominent lately in terms of somebody sending an email to someone in the hopes that they'll download malicious code or other factors. There's, you know, social engineering that takes place in those areas as well. There's—one of the largest categories, though, in the reporting is other. And other includes they don't know what the threat vector was and how people were able to penetrate the system. That is one of the most concerning aspects of this.

Mr. HICE. All right. I want to get there. What are the vectors? When you talk about vectors, what—you've got phishing, you got— what else? What are we dealing with?

Mr. DODARO. Yeah, we have a pie chart in our testimony. Let me just pull that up here.

Ms. KENT. Improper usage, email and phishing.

Mr. DODARO. Right.

Ms. KENT. Loss and theft of equipment and other web-based attacks.

Mr. HICE. Okay. So those comprise more or less 70 percent. Then you mentioned 31 percent——

Mr. DODARO. Right.

Mr. HICE. —other. So does that mean we have no idea how they're breaking in or what they're doing, or what does that mean?

Mr. DODARO. That means that there's—it's unknown, and in some of these cases how these things have occurred. I mean, that's the concerning part of this, and that's one of the points that we make in the report. That's why it's important to have an effort to detect these things when they occur. What's been reported in these cases, I mean, the attacks happen in a matter of minutes, but the detection doesn't occur for months later. And that impairs the ability to determine exactly what happened that led to this attack situation.

Mr. HICE. All right. Ms. Kent, do you want to add to that, your definition or whatever of other?

Ms. KENT. I would just add to the last point that Mr. Dodaro made, is that we have identified that we have to move much more quickly when an attack is identified, to not only share that threat information across agencies, but to act and begin immediate remediation of those issues.

Mr. HICE. All right. Once an attack comes in, particularly, I'm with you, concerned about the other where we have no idea how they're getting in. Is there any way of tracking where they're coming from?

Mr. DODARO. Some of that's possible with some forensics, but in some cases there's not clear audit trails in the systems that are created in the documentation there. One of the big problems, Congressman, here is that, you know, the Federal Government and a lot of agencies are saddled with these legacy financial systems that are like a millstone around their neck. They're old systems. They were designed before security was a prominent area. Some of them at IRS are from the sixties. And so there's not good documentation and, therefore, there's not a good audit trail to follow to figure out how things were introduced.

Mr. HICE. Which is surprising to me and kind of inexcusable seeing that 10 and 10 and 10 of millions of dollars we give for IT on an annual basis around here. It just amazes me that we're still using such legacy systems. It seems like——

Mr. DODARO. Well, of the billions of dollars that you give every year, $80-$90 billion, 75 percent of it goes to maintain these legacy systems.

Mr. HICE. Rather than get updated.

Mr. DODARO. Rather than get updated. That's why we added IT acquisitions and operations across the government as a high-risk area in 2015.

Mr. HICE. My time has expired. Mr. Chairman, thank you so much.

Mr. HURD. The representative from the District of Columbia, Ms. Holmes Norton, you're now recognized for 5 minutes.

Ms. NORTON. Thank you very much.

And I must say, not only do I appreciate our guests appearing, I appreciate the committee for having this hearing, because frankly, I think Americans are increasingly terrified, wondering if anybody is protecting their cybersecurity. And the reason I think so is what we're hearing even on mass media.

This is really an old problem. How many years ago was it this very committee had a hearing on how our Federal employees had been penetrated, and the Congress actually, at that time, gave Fed-

eral employees 10 years of protection against further penetration by way—I'm sure that's running, I'm not sure how long it has to go. I have a bill called the Recover Act. In light of the negligence of the Federal Government, it seems to me that the very least we could do would be to give lifetime coverage. And that's been sufficiently long ago, more than 5 years ago. I think it's going to come up against soon and we're going to be faced with that question for our own employees.

Now, this committee had a recent hearing, and if you want to get—if you want to frighten our people, the head of the DHS, Under Secretary, testified that the Russians were already scanning—it's the word he used—all 50 States. He couldn't tell me that all 50 States, they were doing something in all 50 States. It sounds like reconnaissance. We're looking to see when to hop and whom to hop upon.

So I'm very interested, I think because I represent so many Federal employers that were among those first implicated.

And, Mr. Dodaro, I'd like to ask you about Federal strategy. I'd like to be able to say I left this hearing and I learned something that should put some of my own constituents at ease.

Would you tell me what the Federal strategy is for protecting national cybersecurity here and penetration globally from outside of the United States? Do you have access to such a national strategy?

Mr. DODARO. There are several documents that have been put forward by the executive branch. DHS——

Ms. NORTON. Would you call that a national cybersecurity strategy? And what do you mean by documents? Would you tell us what a document does?

Mr. DODARO. Sure. Sure. Sure. You know—well, first of all, our main point today is there's a need for a more comprehensive national strategy.

Ms. NORTON. There must be something, if you say a more comprehensive——

Mr. DODARO. Right, right. There has been a foundation laid by the government for these strategies. DHS has a strategy that they put forward, they're responsible for coordinating across the Federal Government, and with critical infrastructure protections, and they've laid out a number of components of that strategy. But we found they need—they didn't identify who the—what resources they needed, how they were going to determine they were making progress——

Ms. NORTON. Since several agencies would be involved, who should be in charge of coordinating the development of a strategy—cybersecurity strategy?

Mr. DODARO. Well, it needs——

Ms. NORTON. National cybersecurity strategy.

Mr. DODARO. Yeah. You need to have either an individual or an entity or a process in order to have somebody to coordinate——

Ms. NORTON. For example, with more than a number of agencies involved, who would you suggest? You, the GAO, might be——

Mr. DODARO. Well, it needs to be led out of the White House, in my opinion.

Ms. NORTON. It needs to be led out of the White House. Back and forth.

Mr. DODARO. Because you're dealing with national and global issues in this case.

Ms. NORTON. That's where the coordination needs to happen, and I appreciate that.

Mr. DODARO. Well, it needs to happen at all levels, but the——

Ms. NORTON. Now, somebody needs to be in charge. My concern, Mr. Dodaro, is I can't say to my constituents, don't worry about it. Either some agency is in charge or somebody in the White House is in charge.

What about milestones? Are there at least and what has been put forward by individual agencies, milestones, so that I could say to my own constituents, well, they're this far along and here's an example? That's what people are looking for. Assure me. Reassure me.

Mr. DODARO. No, we would like to see more milestones. DHS has told us, for example, they're working on their strategy, it's supposed to be out next month, that would identify milestones that would include the resources and the performance measures. So we'll wait to see. But that's supposed to be forthcoming.

Ms. NORTON. Ms. Kent, finally, let me ask you, because you are dealing with the IT strategy for the Federal Government. Do you have milestones? And where are we when it comes to helping agencies operationalize these policies so that there is at least governmentwide such an IT strategy? Are they milestones? Who's implementing them? Who's in charge? Are you in charge? You're the chief financial officer, or please detail that.

Ms. KENT. There are indeed milestones, and many of the points that have been made around deployment of continuous diagnostic and monitoring tools, securing agency data, modernizing their technology are part of the milestones that we are tracking. You did see in the report that we are behind across the agencies on some of those. So we have a very specific focus.

There was a milestone set for deployment of the continuous diagnostic and monitoring tools. We have not met that milestone, and we're working very aggressively with the——

Ms. NORTON. What are monitoring tools, please?

Ms. KENT. To be able to—for all of the agencies to have implemented tracking capability so that they know what is on their network.

Ms. NORTON. Yeah. I'm worried about the scanning, for example.

Ms. KENT. Yes. So that we know who is accessing their network——

Ms. NORTON. Yeah.

Ms. KENT. —and what. And so we are working very aggressively with DHS. And one of the critical things that we did as part of the President's Management Agenda was reassess high-value assets. I am pleased to say that we had 100 percent participation from every agency to identify those assets that are most critical, applications and data, and we're working with DHS on those that are most critical for next set of activities.

Ms. NORTON. Thank you very much.

Mr. Chairman, I think the committee needs to do more to press the milestone notion so that we can reassure the American people

that we're getting there and how soon we're going to get there. Thank you very much.

Mr. HURD. Thank you.

The gentleman from Michigan is now recognized for 5 minutes.

Mr. MITCHELL. Thank you, Mr. Chair.

I'd like to pursue a little bit the questioning that my colleague had a few moments ago about these 35,000-plus, quote, incidents. Can you define, Mr. Dodaro, a little more carefully what an incident is, in your interpretation?

Mr. DODARO. I'm going to ask Mr. Wilshusen, our expert in this area, to explain those.

Mr. MITCHELL. Turn your mic on, sir.

Mr. DODARO. Oh, I'm sorry. I'm going to ask Mr. Wilshusen to explain those. He's our expert in that area.

Mr. MITCHELL. Because these aren't—incidents aren't just someone tinkering around trying to scan in your system. Please define them a little more carefully.

Mr. WILSHUSEN. Right. These would be incidents that actually have impacted an agency operation or so. They were able to gain access, and they do this through a number of different mechanisms. One of the more common ones, it's just through what is known as a phishing attack.

Mr. MITCHELL. Phishing, sure.

Mr. WILSHUSEN. In which you send an email with a link and someone clicks on it and it sends them to a——

Mr. MITCHELL. Sends malware.

Mr. WILSHUSEN. —or download some suspicious software.

Mr. MITCHELL. Okay.

Mr. WILSHUSEN. It can also be the loss or theft of equipment that contains sensitive information as well.

Mr. MITCHELL. Sure.

Mr. WILSHUSEN. So there are a number of different types of incidents, but these are ones that do have an impact or can have an impact on the agency.

Mr. MITCHELL. Now, Mr. Dodaro, you referenced earlier that state and non-state actors has been suggested as discussions already started that, again, we're back to Russia. These state actors, examples of state actors impacting our systems go far beyond Russia, do they not?

Mr. DODARO. Yes, they do. I mean, some of the intelligence community has singled out, you know, Russia, China, Iran, North Korea, as you know, actors in this area as well.

Mr. MITCHELL. I'll run the risk of offending some people by saying that I believe occasionally some of our allies actually occasionally are trying to wander around our systems too.

Mr. DODARO. It could be. I mean, I would defer to the intelligence community for those responses.

Mr. MITCHELL. I'll let them get into it. I want to stress, the reality is we face threats both internally and externally through cybersecurity.

When an incident happens, Ms. Kent, how—what's the timeframe by which you're informed we have some level of an incident?

Ms. KENT. There are various timeframes depending on the incident and when the agency identifies the particular activity. Like

you just heard, there's different types of issues and incidents. Some of those may be very quick, others may be a longer timeframe. And as Mr. Dodaro indicated, particularly in situations where there is some type of malware or an attempt to——

Mr. MITCHELL. Let me stop you. I appreciate it. You've got—I understand they can't inform you until they know about them; that's problem one. We'll get to that in a moment. Problem two is that the time from when they have knowledge of the incident, what's the general—what's the expectation—let me change that—what's the expectation that you put out, the White House has put out to inform you that we have an incident of some form? What's the expectation?

Ms. KENT. The expectation is that the agency informed DHS, who is looking at our enterprise risk, and we are tracking all——

Mr. MITCHELL. What's the timeframe on that? Once more, what is the timeframe on that?

Ms. KENT. As immediately as they know.

Mr. MITCHELL. So, theoretically, the same day, next day, that night, whatever the case may be?

Ms. KENT. As quickly as they have identified the incident.

Mr. MITCHELL. When do you find out about it?

Ms. KENT. I find out in reports from DHS?

Mr. MITCHELL. Which is—takes what kind of timeframe?

Ms. KENT. Depends on the type of incident.

Mr. MITCHELL. Go ahead, give me examples.

Ms. KENT. I don't actually have an example.

Mr. MITCHELL. Okay. Let me ask you a question, if I can, Mr. Dodaro. The FISMA audits that are done, in your opinion, are they sufficient, and are actions being taken on those audits at this point in time?

Mr. DODARO. They're a starting point because they're supposed to identify a comprehensive information security system. We find that there are deficiencies in all aspects, access control, segregation duties, configuration management, contingency planning, so—and they're not remedied as quickly as possible. So there are serious security weaknesses that have existed for years, and a number of the FISMA audits at the agencies are in place. But there needs to be more done, because they need to have better response when they find incidents.

Mr. MITCHELL. Who's responsible for those—for that followup?

Mr. DODARO. Well, each agency is responsible for their own actions, and this is an issue, because they're not correcting the problems fast enough, in my opinion. That's why we have it as a designated high-risk area across the entire Federal Government. Virtually every agency has serious weaknesses. And I don't think enough attention's focused by agency managers on getting these areas fixed. We've made recommendations to OMB that they send out more guidance to the agencies to hold senior leaders accountable for getting these weaknesses fixed.

Mr. MITCHELL. One of the things that astonished me, and my time expired here, but let me finish this one comment, Mr. Chair, is that when I first joined Congress and joined this committee, I was astonished by the number of agency chief information officers

that—how do you get someone leading when you've got all of these people doing their own thing? I mean, you——

Ms. Kent, you were in the private sector, and I am short on time so I can't—that didn't happen in your world, now, did it?

Ms. KENT. It did not. And that's also one of the focuses that we have had both under FITARA as well as the recent executive order to have a single CIO that has accountability, responsibility, and visibility across the entire agency, so that we can move the types of things that we were talking about much more quickly.

Mr. MITCHELL. And with that, when there's an incident, they should tell DHS and they should tell you at the same time.

Ms. KENT. Yes.

Mr. MITCHELL. Thank you. I will yield back. Thank you, Mr. Chair, I'm sorry.

Mr. HURD. The distinguished gentleman from Iowa is now recognized for 5 minutes.

Mr. BLUM. Thank you, Chairman Hurd.

Mr. Dodaro, good to see you again. Ms. Kent, good to see you. Thank you for appearing today.

I'm going to change gears a little bit, and I'd like to hear from you your expertise on cloud computing. I understand the Department of Defense is going to have a private company in the private sector host, via the cloud, a lot of government data. And I don't know, my first reaction is, you know, it concerns me a little bit, it concerns people in my district when they hear that. Maybe I shouldn't assume anything.

Do you feel confident that this data will be more secure than if it were with the Federal Government, and why?

Mr. DODARO. Cloud computing offers the potential for, first of all, cost savings, and a more rapidly updating of the systems that are used in place. You know, as we mentioned, you know, these legacy systems have been in the Federal Government for a long period of time, and that's a big problem. If you go to the cloud, then the updating of those systems become the responsibility there.

Now, that being said, there are cost efficiencies and other efficiencies that could be gained. The security is a paramount issue that needs to be addressed. We're looking now, there is a program that's supposed to ensure that there's security over the cloud operations. It's called FedRAMP, is the acronym for it. And we're looking to see if it's an effective tool to make sure there's adequate security in the cloud operations.

Now, the last point I'd make is that the Federal Government's own record of security is pretty abysmal. So, you know, as a starting point—so I don't think, you know, everybody—everybody have a total confidence that everything's fine now, and it may be worse later if we move to the cloud. But you have to be careful in making the move to the cloud environment to make sure there's adequate security.

Mr. BLUM. So more secure is what you feel, I guess?

Mr. DODARO. It could be, but we need to take care to make sure the requirements are there, they're set properly, there's adequate testing, there's certification, there's requirements and operations. It offers a lot of potential for savings, cost savings for the Federal Government, and more up-to-date systems that are better patched

properly and in place. But the security remains as much of a concern with the cloud environment as it does with the Federal agencies, and we need to take due care.

Mr. BLUM. Ms. Kent.

Ms. KENT. Yes, sir. I agree that it can be—it can definitely be secure. And in many cases, it is maintained in a way that we've—we have seen—we have not necessarily done across some of the Federal systems.

I would add two other things to what Mr. Dodaro said, is that there's a discipline around understanding the data and what we're moving to the cloud and how we control access to that. And that is the discipline that we're trying to drive with the agencies as they're considering their transformations and the cloud technologies that they're using. So it's a combination of the security that's available with the technology, what we're putting there, and how we manage access to that information.

And so those are the disciplines that we are—that my office is working directly with the agencies as they consider these acquisitions.

Mr. BLUM. Mr. Dodaro, we often hear things like the Federal Government was slow to respond to an emerging threat, especially cybersecurity threats. What have you found in that regard, and why?

Mr. DODARO. It brings a new definition of slowness, okay. In this area, you know, we first designated it as a high-risk area across the Federal Government in 1997. So I've been trying for over 20 years to get attention to this area. You know, we actually built a computer lab facility that could simulate the operating environment of agencies in the early nineties, and actually did a penetration testing to get people's attention that there could be issues that needed to be dealt with.

And we very, very—it took a long time, but we finally convinced the Congress, legislation began being introduced in 2000, 2002, creating the Federal Information Management Act, the FISMA Act, that was updated. And it really wasn't until the OPM breach that a lot of—in 2015—this is, you know, so many years later that agencies began to move and the administration began to move.

But even then, to this day, I'm not sure OPM has fixed all the weaknesses that led to the original data breach. We went in a couple of times and we haven't found the problem. So it's perplexing to me that there hasn't been enough urgency associated with dealing with this issue. And I'm pleased to hear from Ms. Kent and others that they're going to sort of up the game here to be aggressive in this area.

But there's no question that there has been adequate warnings about these areas that GAO has been given that has been on our top risk list for many years, both within the Federal Government, but also critical infrastructure protection. We put that on in 2003. And concern about the electricity grid, the financial markets, telecommunications, and we're moving in that area, but that's—you know, right now, it's all voluntary on the part of the private sector, and I can understand that, but we need to have a partnership and more information exchange between the private sector and the other sector.

I mean, this is a national security issue, not just, you know, a privacy issue. And privacy has been slow too. You know, we've recommended that the Congress change the—update the privacy laws. The original privacy Act is 1974. E–Government Act in 2002. Many things have changed since then that there needs to be updated information. And while the Congress has only identified some sectors of the economy, healthcare, credit reporting, to put in place rights for consumers about data that's collected about them, there is no consumer privacy framework. We've recommended that Congress consider creating one since 2013.

So, you know, we've been urging for a long time now more attention to this area. I'm glad that we're having this hearing, but I think the pace of change needs to pick up quite a bit, because the threats are evolving way faster than the government's ability to deal with it.

Mr. BLUM. I heard the phrase, and I'll end with this, the warfare of the future may not be bombs, it may be bits and bytes, not bombs. And I know we spend a lot of money on bombs, and we should, but I think we need to give attention to bits and bytes, cybersecurity as well.

Mr. DODARO. Yeah, absolutely. Absolutely. You know, in conventional warfare the first thing people do is take out your communication systems, take out your transportation structure, your ability to have power. But to do that you'd have to physically invade the country. Today that's not exactly the same. You can do it from your own country.

Mr. BLUM. Thank you for your insights. And I yield back the time I do not have, Mr. Chairman.

Mr. HURD. I generally try to have a PMA, a positive mental attitude. My dad taught me that. And I think there has been some bright spots over the last 3–1/2 years since I've been in Congress.

Federal CIOs have more power than they have in the past. They're getting more involved in the procurement process, because we can't hold Federal CIOs accountable if they don't have the responsibilities on what goes on their network. And that's something that this committee has fought for in a very bipartisan way.

I believe when we first started this committee, there were only four CIOs that reported to the agency head or deputy agency head. I think now there's only four that do not. And I believe by the end of the year, there would only be one that is probably not reporting. So, again, empowering the men and women in the CIO.

I've been surprised over the last few months, I've had a number of businesses say that they are happy with improved sharing of intelligence threat information between the Federal and the private sector. Now, that's part of DHS's role, and I think DHS is the only entity that can get into that mode of need to share. And we are seeing what DHS is able to do. And their technical capabilities to help across the other 24 CFO agencies, I think, are improving. And one of the things that is leading to and causing us to see the number of threats increase, because, guess what, DHS is doing their job. Right?

Now, having done this kind of work before, guess what, I'm always going to get in. How quickly can you detect me, How quickly can you quarantine me, and how quickly can you kick me out is

the mentality that we need to be in. But why are some basic things—MEGABYTE Act. The MEGABYTE Act says every agency should know what software they have on their networks. Is that hard to do, Mr. Dodaro?

Mr. DODARO. No.

Mr. HURD. Ms. Kent, is that a hard thing to do to be able to catalog the software that you have on your system?

Ms. KENT. No, sir, we have an opportunity to do much better.

Mr. HURD. And so what is the—what more do we need to do to drive that behavior? Megabyte is important, knowing what your software is, and that's why we've added it on to the FITARA scorecard. The FITARA scorecard is evolving into a digital hygiene scorecard. Naming and shaming is really what we're doing. We're trying to give CIOs the authority with MGT, the Modernizing Government Technology Act, to get out of this notion of if you don't use it, you lose it. So now there's motivation to—motivation to modernize.

What other carrot sticks should we be using or do you need in order to compel compliance on some very basic things, like knowing what software you have?

Ms. KENT. First, I have to applaud and say thank you for the continuous focus on the FITARA scorecard because having that level of transparency does make it a priority.

To your point on MEGABYTE, there are tools and technologies that we can do that with, especially if it's a priority.

One of the things that I would ask that would be of great assistance is the continued focus on workforce activities. In many cases, we still have almost a 25 percent gap in the number of cybersecurity resources that we need across Federal agencies and what we actually have in place. And, particularly, we have some gaps in leadership and individuals—places where we have open positions that are key leaders. In many cases, the individuals, when we get them in, their tenure is less than 12 to 18 months.

So there are multiple workforce actions, both at entry level and at leadership, and there are things that we continue dialogs with the private sector to see if we can fill those gaps.

Mr. HURD. Do we still believe it's—is the number still 15,000, roughly, IT positions that are unfilled across the Federal Government?

Ms. KENT. Yes. Yes, sir.

Mr. HURD. How is the process going to catalog what those positions are? Because we don't have common job descriptions across the Federal Government. This is something that OPM was supposed to be working on. I'd welcome an update on this initiative.

Ms. KENT. We are making good progress on that at clarifying the specific positions, as well as common nomenclature. Particularly, the CIO Council recently published a CISO Handbook to ensure that we are holding our cybersecurity teams accountable for the same standards of behavior across all of the agencies, but we still have work to do to fill those positions. And particularly in the entry levels to ensure that potentially we are identifying other skill sets in the Federal Government that we can move into some of those positions.

Mr. HURD. So when will we have a common picture of what positions are open and what these positions are going to be?

Ms. KENT. I know that it is in the works, and I will get the date back to you.

Mr. HURD. Mr. Dodaro, you mentioned in your written remarks, the national initiative for cybersecurity education, cybersecurity workforce framework. Is that ringing a bell?

Mr. DODARO. It will ring Mr. Wilshusen's, it will ring his bell.

Mr. HURD. It will ring his bell. All right.

Mr. WILSHUSEN. It does.

Mr. HURD. What is that? Where are we—you know, the report recommends, and y'all's report recommends that this is something that is not being addressed properly. Can you give us a little bit more context to this?

Mr. WILSHUSEN. Sure, absolutely. The NIST's Cybersecurity Workforce is an attempt to kind of have a common language and designation for cybersecurity and IT-related activities. And the intent under the Federal Cybersecurity Workforce Assessment Act, Federal agencies are required to assess their cybersecurity workforce, identify the specific functions associated with each of those positions, or their IT and cyber positions, and then assign codes to it in the attempt to identify critical areas of need as it relates to cyber.

We issued a report last month that showed that 13 out of the 23—24 agencies that we examined had not performed all of the activities that they were required to do. And we ended up making about 30 recommendations to those 13 agencies. We have ongoing work continuing—following up on the status of those recommendations and agencies' actions to finish implementation of the requirements of that Act.

Mr. HURD. Good copy. We will come back on a round two. And now, I'd like to recognize my friend from New York, Mrs. Maloney, for her 5 minutes.

Mrs. MALONEY. Thank you very much, Mr. Chairman and Mr. Ranking Member, and all of the panelists.

Mr. Dodaro, in the high-risk report that GAO issued today, it states that the vast number of individuals potentially, if affected by data breaches at Federal agencies and private sector outlets, increases concern considerably that personally identified information is not being properly protected. And I think I agree with you completely too. Given the breaches that we've seen with Verizon in April, they released a report showing that in the past 12 months alone, there was a total over 53,000 incidents, and over 2,200 confirmed data breaches. And then in 2017, we saw the really awful data breach at Equifax, which was over 143 Americans had their personal information stolen. And the 2015 breach at OPM, which affected approximately 22 million individuals. It demonstrates the absolute massive scale of harm to privacy and security that data breaches can have, and this doesn't even get into the alleged foreign governments that are hacking into our private material.

The high-risk reports states, and I quote, that the laws are currently written may not consistently protect personally identified information in all circumstances of its collection and use, end quote.

Can you briefly explain how our current privacy laws and framework for protecting individuals' privacy is not adequate? Obviously, it's not adequate with this large number of breaches taking place. There's some reports that every person in government has been hacked. That everybody's breaking in everywhere. So could you respond to that?

Mr. DODARO. Absolutely. First, the Privacy Act was originally passed in 1974, so it's very dated and did not have anywhere near the context of the current computing environment in place, and what is likely to occur in the future. There was the E–Government Act in 2002 that took a couple of steps, but not sufficient.

Here's two examples. One is that the current definition deals with a system of records that the government's responsibility is protecting that. That doesn't say anything about data mining, it doesn't say anything about databases that are used and scanned and scraped and whatever definition you want to use. So the ability now to be able to manipulate the data doesn't really—is not contemplated under current law.

Second, it gives the Federal agencies the ability to only, you know, use the data for, quote, authorized purposes. Now, that doesn't necessarily give the individuals whose data is being collected an understanding of what is an authorized purpose. So there's really not clarity about what the Federal Government's limits or abilities are to be able to deal with these things.

Mrs. MALONEY. What would you say is an authorized purpose?

Mr. DODARO. Well, it's—every agency is allowed to define it in their own way, which is what——

Mrs. MALONEY. Well, that's not right.

Mr. DODARO. Well, that's what we're saying. Basically, there needs to be more clarity on exactly——

Mrs. MALONEY. Can you get back to the committee with an explanation or a recommended definition of this?

And you went on to say in your report that—that we needed to strengthen our consumer privacy laws. Is that right?

Mr. DODARO. Yes.

Mrs. MALONEY. Could you get back to us on how you would expect us, or to me, on how you'd like us to strengthen it?

And if Congress does move forward with amending and updating the Nation's privacy laws, which we should, what are the key changes that you believe must be achieved?

Mr. DODARO. Yeah. We will definitely provide all that information to you in detail.

On the consumer privacy framework, really, there isn't one, except in the healthcare area and HIPAA, for example, or Federal credit reporting, or some other information—everything—nothing else is really covered, including information reselling of data.

And with other technologies, facial recognition technology and other things, there is no consumer financial privacy—or consumer privacy framework in place, and we recommended that it be put in place. So we can give you some examples of that.

Mrs. MALONEY. Please do. Please do give it.

And I do want to get to OMB for a moment, Ms. Kent. What is the administration's timeline for implementing GAO's rec-

ommendations? Are you implementing these recommendations they put out?

RPTR KEAN
EDTR HUMKE
[3:24 p.m.]

Ms. KENT. We're in process of many of the recommendations, particularly the ones that are in the area of Federal systems and information and, actually, in the privacy and security area that you just talked about.

One of the key elements around how we secure data and citizen data is the efforts under IT modernization.

It is very difficult or complex to secure data in systems that are over 20 years old. And as we modernize, we have better tools for data encryption and management of the data both at rest and in movement, and that is one of the ways that we protect all information that we have within our Federal agency purview against any type of threat.

Mrs. MALONEY. And very briefly, how can Congress assist you in this really huge effort and very, very important one? It used to be privacy was utmost concern on everyone's mind. And now with terrorism, attacks, and other things, it's not taken the really important level that it should in our country. And I want to express my appreciation for your report. But how can we help you?

Ms. KENT. Congress can continue to help us through funding of the teams that focus on these efforts, through creative vehicles like the Technology Modernization Fund that let us actually advance the modernization activities much more quickly, as well as the efforts that I spoke of earlier on workforce.

Mrs. MALONEY. I'm way past time.

Thank you for indulging, Mr. Chairman. I yield back. Thank you.

Mr. HURD. The distinguished gentleman from the Commonwealth of Virginia and ranking member is now recognized for his first 5 minutes of questioning.

Mr. CONNOLLY. Thank you, Mr. Chairman. Thank you for your commitment to this subject matter.

Mr. Dodaro, I want to thank you and GAO for elevating this particular part of the issue to your high risk grouping. Because it forces us to at least talk about it, hopefully do something about it, and you've been instrumental in the past in supporting our FATAR legislation and our scorecard efforts and the like. And I really credit GAO with helping us make the progress we've made.

Last May, the Trump Administration, however, eliminated the White House cybersecurity coordinator position from the National Security Council. In light of your elevation of this as a high risk category, in retrospect, was that a prudent move? Was that a welcome move in the context in which you've delineated this subject matter?

Mr. DODARO. I think, just for clarification, we've had this on the high risk list since 1997, so this isn't a recent elevation. I'm concerned that there hasn't been enough progress in addressing this issue. I was, you know, surprised that the position was eliminated. I've been told that those responsibilities have been divided among two people. I haven't had a chance, since it's a recent activity, to look into it more. We plan to do that in the future.

So once we look into it and see how they're planning to approach it with the elimination of that position, I'll be in a better position to advise the Congress on what to do.

We've never really evaluated this cybersecurity coordinator role. We've been more focused on getting a national strategy in place and making clarifications. And I haven't really examined fully what that position did, what kind of resources they had available and what their accomplishments were during that period of time.

So it's an area that I'm concerned about. You always want to have good leadership, and you can have good leadership in a number of different ways, but I want to look at it more carefully before I advise on exactly what would need to be done differently from what they're contemplating doing.

Mr. CONNOLLY. Yeah, you may be right. I mean, maybe diffusing responsibility or splitting responsibility allows us to have a sum greater—you know, the whole greater than the sum of the parts.

On the other hand, you know, there was a report in Politico that said since its creation in 2009, the White House cybersecurity coordinator position has been key in resolving conflicts among agencies, preparing cabinet leaders to make major policy decisions, and responding to crises.

As you know, Mr. Dodaro, sometimes—maybe more often than not—in government, you need a central focus. You need some champion who is vested with authority and responsibility for moving an agenda, for advocating for a cause. And absent that, often in big bureaucracies, you know, something we all think is a good thing just kind of dies on the vine for lack of attention and championship.

So I would welcome you looking at that because I think we would want to know, did the Trump Administration make a good decision or did it make a mistake in abolishing this position.

Ms. Kent, do you have views on that? I'm sure you do.

Ms. KENT. Sir, I don't know that I would—what I would reflect is that the activities for the Federal agencies are directed by Homeland Security Advisor Fears. And in fact, my chief information security officer has a dual reporting relationship between he and I, so that there is no miss or time in translation for things that we need to take action on.

And I think I have a very clear set of mandates of actions that we need to take across the Federal agencies.

Mr. CONNOLLY. Well, I'm glad to hear that. Do you know how long it took to get a CTO?

Ms. KENT. To get a—I'm sorry?

Mr. CONNOLLY. A chief technology office or a CIO for the Federal Government?

Ms. KENT. Yes, sir, I do.

Mr. CONNOLLY. In this administration, it is over a year.

Ms. KENT. Yes, sir.

Mr. CONNOLLY. So I have to tell you, given that record, it is not exactly confidence-building that, you know, you've got it and you're moving an agenda—not you personally—but the administration. I mean, words are nice but actions are important.

If I may, Mr. Chairman, because I think I'm going to have to run, I have one other subject that is of deep concern to me. And again, I'm going to ask you, Mr. Dodaro, to look into this.

And I agree with what you said, Ms. Kent, we've been champions about the need to upgrade legacy systems or replace them, and to, you know, come into this part of the 21st Century so that we can encrypt, we can protect.

But what is, you know, the purpose of technology is to do the job better. It's to be deployed. It is to give us capabilities we otherwise might not have. One of those capabilities is telework.

And I can tell you as someone who lived through 9/11 and has lived through lots of hurricanes and other kinds of things here in the Nation's Capitol, telework increasingly becomes critical to continuity of operations, without which, government shuts down.

And what has disturbed me is that the Trump Administration seems to be going in exactly the wrong direction with respect to telework. The Department of Education issued new guidelines that seem to severely curtail our robust program.

USDA, which is highly touted by Jared Kushner and Chris Liddell—and I met with them and had a good meeting—but I did bring to their attention that I felt Secretary Purdue was going in the wrong direction on telework. He actually curtailed that program there.

And then your office issued guidelines that, from the White House, that actually would limit, as I understand it, telework to be defined as no more than one day a week.

Now, I don't know anyone in the telework profession who would agree with that definition. No one. Telework is to be encouraged more than one day a week. It's a structured program. It's not a spontaneous, like "gee, I feel like teleworking today." That's not how it works. But we want to get the maximum benefits and we want to deploy technology, and we want to make sure this is part of the offering for the next generation of Federal employee. Because millennials expect that as part of the offering.

So what is going on here in terms of the reluctance to encourage rather than constrain telework in this administration? I have to confess to you, and then I'll shut up, I was really particularly bothered by this because we actually had a good meeting at the White House where we found common ground. And I reassured Mr. Kushner and Mr. Liddell that, frankly, if they continued going in the direction they described they would have our support, which is not an every day occurrence. And then this happened.

And this seems to fly in the face of the kind of progress we thought we were going to make in common.

Ms. KENT. Sir, I'm not informed on the specific decisions that the agencies made around their policies.

I do know that one of the things that we are focused on as part of the President's management agenda and specific goal is the elimination of paper across the various processes in the government to actually free up the ability for individuals to not be dependent on being in a specific physical spot to do that work and drive other efficiencies.

In addition, some of the investments that we're making in digital capabilities and new workforce tools actually enable work to be done from a broader reach of locations.

Mr. CONNOLLY. Well, I mean, there's actually explicit policy guidance that has been drafted that would curtail telework in your administration. And I'll be glad to get it to you, if you haven't seen it.

Mr. Dodaro, I would just ask that you look into this, because I think it flies in the face of the progress we've tried to make. And, you know, the whole point here is to deploy the capability, not constrain it, and would welcome GAO to look into this and see if we can't——

Mr. DODARO. I'd be happy to do so.

Mr. CONNOLLY. I thank you so much. And Mr. Chairman, thank you for your indulgence. I'm sorry.

Mr. HURD. Mr. Mitchell, round two.

Mr. MITCHELL. Thank you, Mr. Chair.

Mr. Connolly, you may want to stay for this conversation—it's the beginning of it—because we're talking about legacy systems.

Mr. Dodaro, have you looked at or done any analysis——

Mr. CONNOLLY. I would say to my friend, I would, but I belong to two committees that believe no human problem cannot be improved with another hearing. And my other committee is practicing that as we speak.

Mr. MITCHELL. Only two committees are doing that? I'm shocked.

It's getting near district work period and it's gone, the wheels have come off the bus around here, okay?

Let's talk about legacy systems for a moment. Have you done any analysis, any examples of the current cost of maintaining legacy systems versus just making a transition to a new system, and what is the comparison?

If you could give me some examples, that would be great.

Mr. DODARO. Well, overall, what we've said of the annual Federal investment, which is about $80, $90 billion a year, 75 percent of that goes to support the legacy systems as opposed to, you know, making investments and modern approaches in systems.

So, you know, we've looked at a lot of individual cases, and I'd be happy to provide those for the record, but, you know, it definitely, you know, the government's track record in implementing new systems and being able to retire legacy systems isn't, you know, very good. But it needs to be better.

And I think the legislation this committee has sponsored is helping move in that right direction. And, you know, I had always approach this with a PMA as well, a positive mental attitude, but I also have a view of what the realistic track record has been of the agencies. I'm hoping they do better. I hope the CIOs will do better in this area, but we need to make a better job in those areas.

So the short answer to your question is the legacy systems involve a lot of spending and are sucking up a lot of the Federal government's investment, and we need to get new systems in place. But every time there's an effort to do that, there's a failure on the part of many agencies.

Now, hopefully with Ms. Kent's leadership and elevating the CIOs to have more responsibility in the agencies, we'll see a different outcome going into the future. I certainly hope so.

Mr. MITCHELL. Well, I would like to see those examples, so if you can get those to the committee with things you've looked at, we would like to look at. Because at some point in time what we're doing is we're paying costs, workforce costs to work on legacy systems that should, in fact, be better——

Mr. DODARO. Yeah, I mean, a good example. We just issued a report about the Coast Guard system that was supposed to be put in place that failed. The VA, they spent, you know, over $1 billion dollars trying to improve the current electronic healthcare system, that hasn't been successful as well.

I mean, we've got a long list of activities where money has been invested, you know, in a lot of cases millions, hundreds of millions of dollars, and it hasn't produced the new system yet properly to retire the legacy system.

So we'll get you a list. I'm confident we have one, and it will touch virtually every agency in the Federal Government.

Mr. MITCHELL. We just had a hearing a bit ago on the Census. And as you are well aware, they are well behind, in terms of developing it's what they do in systems and they're over-budget. So it doesn't surprise me, but we need to start to look at that, so I'd like to see it.

Ms. Kent, could I ask you, you mentioned the vacancies you have, about 15,000 vacancies of technical, cybersecurity personnel; is that connect?

Ms. KENT. Yes, sir.

Mr. MITCHELL. What are the primary drivers of those vacancies.

Ms. KENT. I'm sorry. Say that again?

Mr. MITCHELL. What are the primary drivers, causes of the——

Ms. KENT. Of the vacancies?

Mr. MITCHELL. Yes.

Ms. KENT. The primary drivers of the vacancies is that cybersecurity skills are one of the hottest skills in the industry right now and we're competing with the private sector, as well as the cybersecurity professionals have an expectation of quick mobility, large challenges and some ability to move very quickly in their profession. And some of those things don't align well.

Mr. MITCHELL. We've got big challenges. I can guarantee that.

Ms. KENT. It is a very big challenge, but it's an area where there are many avenues that we're pursuing, both at entry-level positions as well as leadership positions, and continuing to explore exchanges with private sector to fill those gaps.

Mr. MITCHELL. When we had people leave my company, we always did a survey of, kind of get an idea of why you're going. I mean, I'm sure you did as well.

What is the primary—average 10 years about 18 months and they're gone.

What's the primary causes that people are up and leaving once you get them here?

Ms. KENT. It is a highly valuable set of skills in the private sector industry. So many times it is a question of compensation.

What we have to offer is an exciting mission and the ability— we have many very motivated professionals that come in because they believe in the missions that our agencies are focused on.

Other times, they are leaving because they want more mobility. And mobility as they progress through, you know, the professional ranks.

Mr. MITCHELL. Have there been many recognitions made, Mr. Dodaro, on what we do in terms of compensation skill or a career structure for cybersecurity personnel in the Federal system?

Mr. DODARO. No. I mean, this is an area where we've had strategic human capital management on high risk since 2001.

You know, one of the areas——

Mr. MITCHELL. What have you not had on high risk since 2001?

Mr. DODARO. Well, there are things that aren't high risk. You know, we——

Mr. MITCHELL. Okay.

Mr. DODARO. But, you know, the problem here is the classification system that OPM has in place. I mean, there's really not been, I mean that system was created many years ago. It didn't contemplate cybersecurity. They've not adapted over time. And so right now the phase 1 of what the administration is currently doing is to take stock of what cybersecurity skills exists across the government.

I mean, we should have known this for years earlier and developed new systems in place.

Now, Congress has been very good where they've given a lot of special authorities to the agencies. But we found that they have over 100 special hiring authorities but they only use about a dozen or so. And so it's really OPM hasn't looked at whether or not the special hiring authorities are being effective or not.

And so, you know, this means more attention. I'm very glad that the President's reorganization proposals focused on cybersecurity workforce.

Mr. MITCHELL. Can you share with OPM, at least my opinion— not necessarily the committee opinion—but my opinion that—I ran a fair-sized company. The chief technology officer reported to me. They reported to me for a reason. And we had a deal. His phone never went off.

And as soon as something went sideways, you know, he gave warning systems and you're well aware, Ms. Kent, what those are. And the deal was, he immediately went in and dealt with the issues. And the next thing he did was he called me. Because there is nothing that's more important than securing our data.

We're a school group. We have the information on 6,500 students at any point in time, their financial information, their parents' financial information. And that getting hacked is a serious issue, never mind the issues we have here.

So suggest to OPM they may want to up the anti on this and make it a little more important because people aren't trusting the government because they don't believe their data is secure. Never mind the issues it creates for us in terms of national security.

Thank you. I am out of time as well. Thank you, sir.

Mr. HURD. Ms. Kent, one of the recommendations that GAO suggests, needs to be improved, is this global supply chain of information that's on our Federal infrastructure.

So if we take the narrow view of the supply chain of software or hardware that is put on a system responsible in the dot-gov domain, who is responsible for making sure that those widgets are secure?

Ms. KENT. One of the things that I agree with the point around supply chain is ensuring that we have a mechanism, not only to know what is on our network, but to allow Congress and other bodies to make recommendations and have a structured way that we identify both hardware and software, where is it being used, and we have a structured way to pull those things out.

As we worked through the Kaspersky situation, we had to create an entire process, communicate that information, and manage it one-by-one, across all of the agencies. And we did not have a systematic way to do that.

Since we have now had additional concerns and, you know, those may continue, what we would like to have in place is a structured way to do that in ongoing identification by agencies.

Mr. HURD. So let me rephrase the question. Right now can you tell right now agency X, You've got to remove all this stuff? You as the Federal CIO can make that directive and X-agency would have to comply with that.

Ms. KENT. We have been taking directives from the National Security Council or from others, but, yes, that is the way that we have been executing the ones for which we've been given a directive to date.

Mr. HURD. Can the CIO for that agency make that decision and say, All this stuff is coming out?

Ms. KENT. The CIOs have responsibility for the security posture of their agencies, so if they decide to take a more aggressive stance on some situation or, you know, for some reason that aligns with their mission, that is within their authority.

Mr. HURD. So let's say an agency has a device on their network that they shouldn't have, who should be in trouble? Who is responsible for having allowed that to happen? Or not finding that out in advance?

Ms. KENT. That's a good question. We do hold agencies accountable for knowing what is on their network. And if there has been a directive to remove actions and a specific date by which to act, we are holding them accountable from an oversight perspective.

Mr. HURD. Mr. Dodaro, do you have any opinions on this?

Critical infrastructure, I mean excuse me, supply chain within the dot.gov space. Let's start with that.

Mr. DODARO. Yeah, right, right. I think, you know, individual agencies are always the first line of responsibility in these cases to know what they're buying and what is in place.

DHS has responsibility and has the ability to issue binding operational directives to agencies, across government, if need be, to remove devices or to do certain things as well. So DHS has some responsibilities.

I would ask Greg to come up. He just testified on a supply chain issue recently, see if he has any additional thoughts.

Mr. HURD. While he is coming up, describe your vision, the future state that needs to happen in order for this to be removed from the GAO high risk report.

Mr. DODARO. On supply chain or the whole——

Mr. HURD. On supply chain over dot-gov.

Mr. DODARO. Yeah, there needs to be, you know, a clearer plan for determining the supply chain operations, you know, in terms of identification of vulnerabilities, and there needs to be greater accountability for enforcing that over time.

Mr. HURD. Who should do that?

Mr. DODARO. It has to be led by DHS or out of the White House to be enforced. I mean, it has to be. I mean, you know—and there are separate issues at DOD, all right, on this issue, you know, for national security purposes, and they hold the prime contractors responsible. But there is a lot of subcontractors kind of issues.

But in the civilian side of the government, I think it's got to come from DHS primarily, would be where I would start.

Mr. HURD. Mr. Wilshusen.

Mr. WILSHUSEN. Yeah. It would need to be, I think, also DHS, but also certainly with input, collaboration with the intel community as well as DOD as they collect intelligence and information about the particular supply chain direct to particular components or systems that might be in use at Federal agencies.

DHS has used its authority under the Federal Information Security Modernization Act to issue binding operational directives to require and compel all Federal agencies to remove Kaspersky Lab-type products, as was referenced earlier.

We have been requested and we plan to start an engagement later this year to look at the process by which DHS determines when to issue a binding operational directive, how it comes about that decision and then what oversight mechanisms it has to ensure that its directives are actually being implemented and implemented effectively by the agencies.

Mr. HURD. Shifting gears on privacy. If the IRS database got hacked—and let's say a portion of American citizen's information was stolen—what is the responsibility of IRS to notify those individuals and notify Congress?

What is the breach notification rules that IRS would be following in that case?

Mr. WILSHUSEN. It depends. IRS would need to make—and this is under guidance provided by the Office of Management and Budget, indeed on how to respond to particular data breaches.

Part of it is to conduct, at first, a risk assessment in which it looks at the scope of the breach and the potential harm that could occur to, say, in this case taxpayers, if their information is indeed compromised.

And then it's supposed to make a risk assessment and then determine what type of actions to take. Part of that could include notification to those individuals that their information has been breached. It could also include providing some other remedies such as credit monitoring services and others——

Mr. HURD. So this is the standard written by OMB?

Mr. WILSHUSEN. That's correct.

Mr. HURD. So if students' loan information at Department of Education was stolen, would that be the same notification responsibilities and privacy——

Mr. WILSHUSEN. Yes, those guidelines are for all Federal agencies.

Mr. HURD. So OMB has issued breach standard notification across the Federal Government to include intel and militaries across all Federal agencies or is it just the dot-gov space?

Mr. WILSHUSEN. I guess it would be dot-gov space.

Mr. HURD. Ms. Kent, do you have any opinions on this topic?

Ms. KENT. It is not a topic that I am familiar with, all the specifics. I do recognize, though, in the description is, the process is very similar to industry and the notification process, identifying risks, understanding the risk of the individuals, and then determining if there are other mitigating factors that should be offered to those individuals.

Mr. HURD. Ms. Kent, changing gears here. OMB released its agency self-reported data on the status of their information security controls. We have found that agencies tend to present a prettier picture than their own IGs in those FISMA audits.

Have you noticed this discrepancy? Are you working to make this accurate reporting? Are you acknowledging these problems? How do we plan to work with agencies to implement some of these basic cybersecurity requirements.

Ms. KENT. I concur with your assessment. That was actually when I looked at the reports, one of the early things that I asked in joining.

It is actually a conversation that I have had with the GAO team about how we can automate and actually extract data on some of the specific points versus asking for a self-reporting mechanism. And we'll continue the dialogue about how to improve that.

Mr. HURD. This is one of my final questions. It's a very broad basic question, and it's broad and basic for a reason. And we'll start with you Ms. Kent, and then we'll go down the line.

Who is responsible for defending the digital infrastructure of the Federal Government?

Ms. KENT. Say that again?

Mr. HURD. Who is responsible for defending the digital infrastructure of the Federal Government?

Ms. KENT. The agencies are responsible for defending the digital infrastructure at their agency, and DHS is responsible for defending across the enterprise. And there's an interlock of responsibilities between the agencies and their communication with DHS in ensuring that DHS has visibility to issues, incidents, and what they are detecting going on in those individual agencies.

Mr. HURD. What is the role of the Federal Government in helping to defend the 16 areas that we consider to be critical infrastructure?

Ms. KENT. I don't know that I'm following your question. Are you talking about the external industry?

Mr. HURD. So the 16 areas that we think are critical infrastructure, financial services, utilities, election infrastructure, go down the line, what is the Federal government's role in helping to defend those infrastructures?

Ms. KENT. I see those as the responsibility of DHS. So I don't know that I am informed to comment. DHS and our National Security Council. And from a Federal agency perspective, I know when we expect that they are sharing threat information from those industries with us inside the Federal agency side so that we can react to those.

Mr. HURD. Got you. Mr. Dodaro, who's in charge?

Mr. DODARO. Well, in the Federal space, I would agree. I mean, the agencies are primarily responsible according to FISMA. That's the agency heads. I mean, Congress has established that in law. It has given DHS responsibility and law. And OMB sort of passed that responsibility to DHS years ago and without the authority.

Now, Congress corrected that and gave DHS the authority, gives them the ability to issue these binding operational directives. And then OMB has responsibility as well for policy matters in a lot of these areas.

So in the Federal space, I think that's pretty clear. In the critical infrastructure protection space, less so.

Now, in some of the critical infrastructures, for example, in the nuclear area, there are regulatory responsibilities. So the Federal government's role is a little clearer in that area. They have more authority to put in place requirements. But for by and large, for most of the 16 sectors for critical infrastructure, it's voluntary.

And what we found is that the—there each has a Federal coordination point and a lot of the Federal coordinators really didn't know what the status was of the implementation of the voluntary standards.

When we talked to a number of people in the sectors, you know, they were basically saying that they had challenges. They didn't have enough people, they didn't understand all the requirements. So that's the area I'm most concerned about.

Mr. HURD. So describe that future state when it comes to critical infrastructure that if we achieved you would pull this off as one of the four major challenges facing the Federal Government.

Mr. DODARO. Yeah. Well, number one, I would have to have some metrics and measures to know what the state of readiness really is in those areas.

Right now, you don't have that. No one can answer that question, I believe, to say across the 16 sectors were ready. And here is why I believe that.

So to me, you need that in place to provide the level of assurance that would be necessary in order to do that. And so that's, you know, a tall order. And then you would need to have, you know, a clearer understanding of information sharing.

You know, our understanding of what's going on, you referenced this earlier about businesses being happy with information they're getting from DHS. I'm not too sure that that information flow is going two ways. And I think we need to, from the Federal Government standpoint, need to have greater assurance that there's a two-way dialogue here, and that we're really communicating and understanding what's going on with the risk in those areas.

So to me, you need a clear metric understanding of what the status of readiness is for each of the 16 areas, and there would be different metrics for different sectors. I'm not suggesting there would

just be one sector, but somebody has got to be in that position to know that.

And right now, that's very sketchy at best. And as a result, I think we're very vulnerable in the Nation. I know there's a lot of policy issues about the Federal role, respecting the private sector, whatever. But I think we're getting to a point with the threats from state and non-state actors that we need to have more of a grownup conversation about the real risk to the country in those areas and a meeting of the minds on how best to protect our country for everybody.

Mr. HURD. Has GAO thought through what are those Doomsday scenarios that we should be prepared for? Because if there are unclear roles between the public and private sectors in response to a Doomsday scenario, we need to be thinking through what are those Doomsday scenarios that we need to be prepared for.

Have you all spent some time on that? Have you all seen an entity that has designed that?

Ms. Kent, you have seen stuff?

I know there are some exercises. DHS does a few. But I feel like we haven't done enough, because if we're truly going to escape to a future state, we need to figure out what that is we're trying to be prepared for.

If we're going to develop contingency planning, what contingency are we planning for?

And Mr. Wilshusen you came up here, so I hope you have some interesting things to say.

Mr. WILSHUSEN. I hope I can interest you.

One, is DHS has developed a response plan, and it's tested annually, in which it is a test against different types of scenarios.

And I do believe in some of the guidance at least—well, from the National Institute of Standards and Technology and some of its guidance, it does identify different threat scenarios for different types of potential attacks that can affect organizations and systems.

Now, that's generally guided towards Federal agencies, but those same types of attacks can also be applied against critical infrastructure owners and operators in the systems that they operate.

And so there are different threat scenarios that have been identified and those are things that both I think DHS and NIST has identified.

Mr. HURD. Well, Mr. Dodaro, you've heard me say this before. I'm a big fan of GAO. Whenever there's a new topic I am working on, I always start with whatever reports you all have developed.

So thank you for you and your team and you all's service to making sure our government is responsive to the people that we serve. It's always a pleasure to have you here.

Ms. Kent, any final words?

Ms. KENT. I thank you for the opportunity. And as I said in the opening, every chance that we have to elevate the conversation around cybersecurity and the resources that we need to be in a position to protect our security posture, I greatly appreciate.

Thank you.

Mr. HURD. Well, I thank our witnesses for appearing before us today.

The hearing record will remain open for two weeks for any member to submit a written opening statement or questions for the record.

And if there's no further business, without objection, the subcommittee stand adjourned.

[Whereupon, at 4:01 p.m., the subcommittee was adjourned.]

APPENDIX

———————

MATERIAL SUBMITTED FOR THE HEARING RECORD

House Committee on Oversight and Government Reform

Committee Hearing:

GAO's High Risk Focus – Cybersecurity

Questions for the Record

Questions for the Record from Gerald E. Connolly, Ranking Member, Subcommittee on Government Operations

1. **Regarding the White House's decision to eliminate the White House Cybersecurity Coordinator position from the National Security Council in May 2018: In its special mid-cycle high-risk report on cybersecurity, the Government Accountability Office (GAO) reported that it had recommended that "the White House Cybersecurity Coordinator in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy."[1]**

   a. **Please explain how having a Cybersecurity Coordinator at the White House level, would be beneficial to the federal government's efforts to develop a more effective, government-wide cybersecurity strategy?**

   The White House Cybersecurity Coordinator position was created in December 2009 to, among other things, coordinate interagency cybersecurity policies and strategies, and to develop a comprehensive national strategy to secure the nation's digital infrastructure. In reporting on federal efforts to establish a national strategy in 2013, we highlighted specific roles and responsibilities that had been assigned to the Coordinator, including being designated as the leader for implementing cost-effective and efficient cybersecurity controls for federal information system security.[2] Further, we noted that the Coordinator was the lead for the development and implementation of a public awareness strategy and a strategy for better attracting cybersecurity expertise and increasing cybersecurity staff retention within the federal government. These responsibilities

---

[1]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-645T (Washington, D.C.: July 25, 2018).

[2]GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

continue to be critical to ensuring that effective leadership and oversight are provided as part of developing and implementing a national cybersecurity strategy.

b. **What is GAO's assessment as to how the elimination of the Cybersecurity Coordinator role could potentially affect implementation of its recommendation that the federal government "develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace?"[3]**

With respect to our prior recommendation, it is vital that the executive branch clearly define roles and responsibilities (including cybersecurity leadership) in order to develop and implement a more comprehensive national cybersecurity strategy. My recent testimony noted that the various strategy related documents that the government has issued lack clearly defined roles and responsibilities, such as those activities that had been assigned to the Coordinator position prior to its elimination. For example, although the National Security Strategy discusses multiple priority actions needed to address the nation's cybersecurity challenges (e.g. building defensible government networks and deterring and disrupting malicious cyber actors), it does not describe the roles, responsibilities, or the expected coordination of any specific federal agencies, including the Department of Homeland Security, the Department of Defense, or the Office of Management and Budget, or other non-federal entities needed to carry out those actions.

We plan to initiate a review by the end of calendar year 2018 that is to examine cybersecurity roles and responsibilities across the federal government, including within the Executive Office of the President.

c. **Does the nature of the cybersecurity threats our nation is presently facing lend itself to having an individual at the White House level who has centralized and broad authority for coordinating the nation's overall cyber strategy**

      i. **If so, please explain why.**

As emphasized in my testimony, the risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. [4] As such, clearly identifying the federal officials and executive branch entities that are responsible for developing and implementing a national strategy is essential to overcoming the cybersecurity challenges that we have identified. These challenges include, for example, maintaining a qualified cybersecurity workforce, addressing security weaknesses in federal systems, and improving cyber incident response efforts. Without clearly defining the roles and responsibilities of key entities, such as the White House, the federal government may not be able to foster effective coordination and hold agencies accountable for carrying out planned activities to address the challenges we identified.

---

[3] GAO-18-645T.

[4] We first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

d. Should the Cybersecurity Coordinator role not be reinstated by the White House, what recommendations does GAO have for ensuring that the federal government develops a more comprehensive strategy for dealing with cyber threats?

In the absence of a Cybersecurity Coordinator position, it is still of utmost importance that roles and responsibilities be clearly defined in order to achieve a more comprehensive national strategy. As I pointed out in my testimony, recent executive branch actions to document cybersecurity efforts across the federal government provided a good foundation for a comprehensive cybersecurity strategy, but more effort is needed to address all of the desirable characteristics of a national strategy that we previously recommended. In addition to the fact that most of the current executive branch strategy documents lack clearly defined roles and responsibilities for key agencies that contribute substantially to the nation's cybersecurity programs, these strategy documents generally do not include milestones and performance measures to gauge results of the activities intended to meet the stated cybersecurity goals. Further, the strategy documents generally do not include information regarding the resources needed to carry out activities to meet the goals and accomplish the objectives. Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

We plan to initiate a review of cybersecurity roles across the federal government by the end of calendar year 2018. As part of that review, we plan to evaluate what actions have been taken to mitigate the aforementioned challenges and determine what, if any, additional steps are necessary for the federal government to develop more comprehensive strategy for dealing with cyber threats.

Questions for Ms. Suzette Kent
Federal Chief Information Officer
U.S. Office of Management and Budget

Questions from Representative Gerald E. Connolly, Ranking Member
Subcommittee on Government Operations

July 25, 2018, Hearing: "GAO High Risk Focus: Cybersecurity"

1. Regarding the White House's decision to eliminate the White House Cybersecurity Coordinator position from the National Security Council in May 2018: In its special mid- cycle High-risk report on cybersecurity, the Government Accountability Office (GAO) reported that it had recommended that "the White House Cybersecurity Coordinator in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy."[1]

   a. In light of the White House's decision to eliminate the role of White House Cybersecurity Coordinator, who at the White House level has broad authority and responsibility for coordinating cybersecurity strategies across the federal government?

   The Assistant to the President and National Security Advisor has the broad authority and responsibility for coordinating cybersecurity strategies across the federal government. With respect to non-national security systems at federal agencies, the Director of the Office of Management and Budget has the authority and responsibility for overseeing agency information security policies and practices.

   b. Were you consulted beforehand about the decision to eliminate this position?

   I was not.

○