THE CURRENT STATE OF DHS'S EFFORTS TO SECURE FEDERAL NETWORKS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 28, 2017

Serial No. 115–10

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

26–908 PDF WASHINGTON : 2017

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
KATHLEEN CROOKS FLYNN, *Deputy General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

JOHN RATCLIFFE, Texas, *Chairman*

JOHN KATKO, New York
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
VAL BUTLER DEMINGS, Florida
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
K. CHRISTOPHER SCHEPIS, *Minority Staff Director*

CONTENTS

THE CURRENT STATE OF DHS'S EFFORTS TO SECURE FEDERAL NETWORKS

Tuesday, March 28, 2017

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

The subcommittee met, pursuant to notice, at 10:10 a.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe (Chairman of the subcommittee) presiding.

Present: Representatives Ratcliffe, McCaul, Katko, Donovan, Gallagher, Fitzpatrick, Richmond, Thompson, Jackson Lee, Langevin, and Demings.

Mr. RATCLIFFE. Good morning. The Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection will come to order. The subcommittee is meeting today to receive testimony regarding the current state of the Department of Homeland Security's efforts to secure Federal networks. I recognize myself for an opening statement.

I see cybersecurity as one of the preeminent domestic and National security policy challenges of our generation. As the Chairman of the Cybersecurity and Infrastructure Protection Subcommittee, I feel especially grateful for the opportunity to work with other Members on this panel to have a direct impact on the cybersecurity posture of our country.

This is a duty that we do not take lightly. Oftentimes, the American people hear about committees performing oversight. They think there is this misguided perception that we are simply performing a routine check-up, taking the temperature, if you will, and then moving on.

That mindset isn't what compels us to meet here today. Today's oversight is one of committed on-going engagement. Securing Federal networks is, and rightfully should be, one of the central priorities of this subcommittee, of this committee, of this Congress, and for the American people.

While today's hearing represents a small public-facing sliver of this engagement, my commitment to all stakeholders impacted by this important issue is that our continued efforts to improve the security of our Federal networks will be conducted in a manner that fully recognizes the seriousness of the threats posed by our cyber adversaries. While the stakes are indeed high, this subcommittee is uniquely positioned to be part of the solution.

After all, the Department of Homeland Security is required by law to play a vital and central role in the Federal Government's policy, procedures, and operations for cybersecurity of our Federal agencies.

Specifically, DHS is entrusted with carrying out important legislative priorities established by the Cybersecurity Act of 2015 and the Federal Information Security Modernization Act of 2014, often referred to as FISMA.

Ensuring the effective execution of the Department's cybersecurity initiatives has never been more important than it is today. Just last week, the committee heard from a panel of experts about the evolving cyber landscape.

Retired General and National Security Advisor Keith Alexander, noted "Our increasing reliance on digital connected devices means that, while tanks, bombers, and fighter jets are certainly not obsolete, there are newer and perhaps more insidious ways of having similar effects without the need for a large investment that those assets require."

Bad actors are continuing to compromise the network security of both the public and the private sectors at an alarming rate. From nation-states like Russian, China, Iran, and North Korea and criminal organizations, our systems are regularly attacked, and the Federal Government must be more effectively and more efficient in anticipating these threats and do a better job of protecting itself and the vast troves of sensitive information on its networks.

According to law, DHS is required to provide intrusion detection and prevention capabilities to Federal agencies and to work with the Office of Management and Budget to administer the implementation of agency information security policies and practices. The Department must include advanced network security tools in its efforts to continuously diagnose and mitigate cybersecurity risks.

Additionally, DHS has the authority to issue binding operational directives to Federal agencies in order to safeguard Federal information and information systems. The Department's perimeter defense capabilities, known as EINSTEIN, have progressed from monitoring to detection to actual prevention capabilities.

A pilot is under way to examine detection technologies beyond signature-based detection, as required by the Cybersecurity Act of 2015. While questions about the time line of full deployment of the Continuing Diagnostics and Mitigation program, or CDM, phases loom, breaking down initial barriers to provide agencies with real-time situational awareness and risk-based accountable information is imperative to our Federal cybersecurity efforts.

I look forward to hearing from our witnesses today about the current status of these programs and how they will provide greater security for Federal information technology systems, when they are fully deployed.

In today's ever-changing cyber threat landscape, we need to ensure that these programs are agile enough to keep pace with the cybersecurity needs of our Federal agencies.

We need to ensure that DHS is properly leveraging private-sector innovation and is able to quickly adopt cutting-edge technologies. We need to ensure that there is a comprehensive strategy in place,

not only to engage every Executive branch agency and Department, but also to ensure coordinated deployment.

The Federal Government requires the American people to submit sensitive information to its care, private financial information to the IRS, personal medical records to Medicare or to the VA. We often adopt a trust-us approach, but if we require that, then I firmly believe we must take serious steps to demonstrate our trustworthiness with that information.

I look forward to a productive conversation with this distinguished panel of witnesses. Working together, we can continue to strengthen DHS's cyber capabilities to secure our Federal networks.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

MARCH 28, 2017

I see cybersecurity as one of the pre-eminent domestic and National security policy challenges of our generation, and as the Chairman of the Cybersecurity and Infrastructure Protection Subcommittee I feel especially grateful for the opportunity to work with the other Members on this panel to have a direct impact the cybersecurity posture of our country. It's a duty we do not take lightly.

Oftentimes when the American people hear about committees performing oversight, there's a misguided perception that we're simply performing a routine checkup, taking the temperature if you will, and then moving on.

That mindset is not what compels us to meet here today.

Today's oversight is one of committed, on-going engagement. Securing Federal networks is—and rightfully should be—one of the central priorities of this subcommittee, of this Congress, and for the American people. While today's hearing represents a small, public facing sliver of this engagement, my commitment to all stakeholders impacted by this important issue is that our continued efforts to improve the security of Federal networks will be conducted in a manner that fully recognizes the seriousness of the threats posed by our cyber adversaries. And while the stakes are indeed high, this subcommittee is uniquely positioned to be part of the solution.

After all, the Department of Homeland Security is required, by law, to play a vital and central role in the Federal Government's policies, procedures, and operations for the cybersecurity of our Federal agencies.

Specifically, DHS is entrusted with carrying out important legislative authorities established in the Cybersecurity Act of 2015 and Federal Information Security Modernization Act of 2014.

Ensuring the effective execution of the Department's cybersecurity initiatives has never been more important than it is today. Just last week, the committee heard from a panel of experts about the evolving cyber threat landscape. Retired General Keith Alexander noted, "Our increasing reliance on digital, connected devices means that while tanks, bombers, and fighter jets are certainly not obsolete, there are newer and perhaps more insidious ways of having similar effects without the need for the large investment that those assets require."

Bad actors continue to compromise the network security of both the public and private sectors at an increasingly alarming rate. From nation-states like Russia, China, Iran, and North Korea and criminal organizations our systems are regularly attacked and the Federal Government must more effectively and efficiently anticipate these threats and do a better job protecting itself and the vast troves of sensitive information on its networks.

According to law, DHS is required to provide intrusion detection and prevention capabilities to Federal agencies and work with the Office of Management and Budget to administer the implementation of agency information security policies and practices. The Department must include advanced network security tools in its efforts to continuously diagnose and mitigate cybersecurity risks. Additionally, DHS has the authority to issue Binding Operational Directives to Federal agencies in order to safeguard Federal information and information systems.

The Department's perimeter defense capabilities, known as Einstein, have progressed from monitoring, to detection, to actual prevention capabilities. A pilot is under way to examine detection technologies beyond signature-based detection, as

required in the Cybersecurity Act of 2015. And, while questions about the time line for full deployment of Continuous Diagnostics and Mitigation Program—or CDM—phases loom, breaking down the initial barriers to provide agencies with real-time situational awareness and risk-based accountable information is imperative to our Federal cybersecurity efforts.

I look forward to hearing from our witnesses today about the current status of these programs and how they will provide greater security for Federal information technology systems when fully deployed.

In today's ever-changing cyber threat landscape we need to ensure that these programs are agile enough to keep pace with the cybersecurity needs of Federal agencies. We need to ensure DHS is properly leveraging private-sector innovation and is able to quickly adopt cutting-edge technologies. We need to ensure that there is a comprehensive strategy in place, not only to engage every Executive branch agency and Department but also to ensure coordinated deployment.

The Federal Government requires the American people to submit sensitive information to its care—private financial information to the IRS, personal medical records to Medicare or the VA. We often adopt a "trust-us" approach. But if we require that, then I firmly believe we must take serious steps to demonstrate our trustworthiness.

I look forward to a productive conversation with our distinguished panel of witnesses. Working together we can continue to strengthen DHS's cyber capabilities to secure Federal networks.

Mr. RATCLIFFE. The Chair now recognizes the Ranking Minority Member of our subcommittee, the gentleman from Louisiana, Mr. Richmond, for his opening statement.

Mr. RICHMOND. Thank you Mr. Chairman. Thank you to the Chairman of the full committee and the Ranking Member of the full committee for being here.

I want to begin by thanking you for holding this hearing on one of our Nation's most pressing homeland security challenges, and that is securing the dot-gov domain.

Americans rely on Federal agencies to safeguard some of our most sensitive National data, from health records and Social Security numbers, to intelligence and information on our troop movements. This information may be exposed or exploited by something as simple as a careless employee or a failure to patch a known vulnerability.

This information can just as easily be taken or altered by criminal networks and, as we discussed last week in this committee, state-sponsored hackers. The Russian attacks this past year on our democratic processes and political institutions are a salient reminder of the damage state adversaries, like Russia, can inflict.

Just last year, the GAO surveyed agencies with high-impact systems, those that hold information so sensitive that a breach could cause catastrophic harm to individuals, the Government, or the Nation. The survey showed that cyber attacks from state actors represented the most serious and frequent threat these agencies faced.

This same team of GAO analysis, one of whom we have with us today, revealed that from 2006 to 2015, the number of cyber attacks on Federal agencies went from about 5,500 per year to 77,000. That is a 1,300 percent increase.

We also know that our Government networks have not only been targeted, they have also been infiltrated. Successful cyber attacks have been carried out against the Office of Personnel Management, the Internal Revenue Service, and the Departments of State, Defense, Veteran Affairs, and Health and Human Services, just to name a few.

To be clear, there is no one-size-fits-all or a silver bullet for securing Federal networks. That said, there are some positive signs that current efforts may be having an impact.

A recent report from the Office of Management and Budget shows that over the last year the number of cyber attacks on the United States Government networks have gone down, not up, for the first time in a decade.

I am also interested to hear from DHS and GAO on the extent to which this downward trend may be attributable, at least in part, to greater adoption of the EINSTEIN program by Federal agencies.

I also look forward to hearing from this panel about how DHS is working with its Federal partners to deliver cybersecurity services that are valuable, affordable, and effective.

With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC RICHMOND

MARCH 28, 2017

Americans rely on Federal agencies to safeguard some of our most sensitive National data—from health records and Social Security Numbers to intelligence and information on troop movements.

This information may be exposed or exploited by something as simple as a careless employee or a failure to patch a known vulnerability.

This information can just as easily be taken or altered by criminal networks and—as we discussed last week in this committee—state-sponsored hackers.

The Russian attacks this past year on our democratic processes and political institutions are a salient reminder of the damage state adversaries like Russia can inflict.

Just last year, GAO surveyed agencies with "high-impact" systems—those that hold information so sensitive that a breach could cause catastrophic harm to individuals, the Government, or the Nation. The survey showed that cyber attacks from state actors represented the most serious and frequent threat these agencies faced.

This same team of GAO analysts, one of whom we have with us today, revealed that from 2006 to 2015, the number of cyber attacks on Federal agencies went from about 5,500 per year to over 77,000—a 1,300% increase.

We also know that our Government networks have not only been targeted, they have also been infiltrated.

Successful cyber attacks have been carried out against the Office of Personnel Management, the Internal Revenue Service, and the Departments of State, Defense, Veterans Affairs, and Health and Human Services, to name just a few.

To be clear, there is no one-size-fits-all, "silver bullet" for securing Federal networks.

That said, there are some positive signs that current efforts may be having an impact. A recent report from the Office of Management and Budget shows that, over the last year, the number of cyber attacks on U.S. Government networks has gone down—not up—for the first time in a decade.

I am also interested to hear from DHS and GAO on the extent to which this downward trend may be attributable, at least in part, to greater adoption of the EINSTEIN program by Federal agencies.

I look forward to hearing from this panel about how DHS is working with its Federal partners to deliver cybersecurity services that are valuable, affordable, and effective.

Mr. RATCLIFFE. Thank the gentleman.

The Chair now recognizes the Chairman of our full committee, my colleague from Texas, Mr. McCaul, for an opening statement.

Chairman MCCAUL. Thank you, Mr. Chairman and Ranking Member. I want to thank the subcommittee for the good work that you have been doing, not only last Congress, but I know we have a lot of work to do in this Congress. I look forward to that.

Just last week, our committee heard from top former cyber and National security officials, including General Keith Alexander, that we must rise to the challenge in combatting growing cyber risk, and that we must up our game on our defense. We heard about the wide range of cyber threats we face from nation-states, hacktivists, and criminals.

Russia meddled in the 2016 Presidential election and Russian intelligence agents were indicted in the massive breach of Yahoo. North Korea attacked Sony Pictures. Iran hit the financial sector.

China continues to be one of the Nation's top cybersecurity threats. As we all remember in 2015, Chinese hackers stole 20 million security clearances, including my own, and many in this room, in a breach at the Office of Personnel Management.

Recently, the alleged hack of the CIA has WikiLeaks publishing over 8,000 pages of documents with some of the most highly sensitive cyber weapons.

These blinking red alarms are the reason we are here today. We need to ensure that our Federal departments and agencies are properly defended from attacks. We do not have time to wait.

Over the last several years, I have championed a number of bills out of this committee that put DHS in the lead for operational control and to operationally secure the dot-gov domain, helping to better protect critical infrastructure, hiring cyber talent at MPPD, being the hub for the cyber threat information sharing and providing voluntary assistance to the private sector.

In late 2015, the Cybersecurity Act became law, and included language authorizing DHS to deploy intrusion detection and prevention capabilities and to support its continuous diagnostics and mitigation endeavors across the Federal civilian enterprise.

This law requires Federal agencies to utilize the intrusion detection and prevention capabilities. At the end of last year, the Department announced it was providing cybersecurity services to 93 percent of the Executive branch's civilian work force.

But perimeter detection is only one part of what needs to be a larger part and more holistic defense-in-depth strategy and architecture. DHS must adopt an entire suite of tools and technologies while ensuring its capabilities are keeping up with the evolving cyber threats that we discussed at last week's hearing.

As I mentioned last week, this committee will be moving legislation soon to create a stronger, consolidated cybersecurity agency at the Department of Homeland Security.

This proposal will elevate the cybersecurity mission at DHS at a critical time and further enhance cyber operations, including those to more effectively secure Federal networks. This will help step up our cyber defense efforts and attract top talent, as we have already begun to work with DHS and others to make that a reality.

So I want to thank the Chair and Ranking Member for holding this hearing. I look forward to seeing the testimony. With that, I yield back.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

MARCH 28, 2017

I look forward to hearing from our witnesses today on this essential aspect of the DHS cybersecurity mission, protecting our Federal civilian networks.

Just last week, our Committee heard from top former cyber and National security officials, including General Keith Alexander, that we must rise to the challenge in combating growing cyber risks and that we must up our game on defense.

We heard about the wide range of cyber threats we face from nation-states, hacktivists, and criminals.

Russia meddled in the 2016 Presidential election and Russian intelligence agents were indicted in the massive breach of Yahoo.

North Korea attacked Sony pictures.

Iran hit the financial sector.

China continues to be one of the Nation's top cybersecurity threats and, as we all remember, in 2015, Chinese hackers stole 20 million security clearances—including my own—in a breach of the Office of Personnel Management.

And, recently, the alleged hack of the CIA has Wikileaks publishing over 8,000 pages of documents with some of the most highly sensitive cyber weapons.

These blinking red alarms are the reason we are here today. We need to ensure that our Federal departments and agencies are properly defended from attacks; we do NOT have time to wait.

Over the last several years, I have championed a number of bills that put DHS in the lead for operationally securing the "dot-gov" domain, helping to better protect critical infrastructure, hiring cyber talent at NPPD, being the hub for cyber threat information sharing, and providing voluntary assistance to the private sector.

In late 2015, the Cybersecurity Act became law and included language authorizing DHS to deploy intrusion detection and prevention capabilities and to support its continuous diagnostics and mitigation endeavors across the Federal civilian enterprise.

The law requires Federal agencies to utilize the intrusion detection and prevention capabilities and at the end of last year, the Department announced it was providing cybersecurity services to 93 percent of the Executive branch's civilian workforce.

But perimeter detection is only one part of what needs to be a larger and more holistic defense-in-depth strategy and architecture.

DHS must adopt an entire suite of tools and technologies while ensuring its capabilities are keeping up with the evolving cyber threats that we discussed at last week's cyber threat hearing.

As I mentioned last week, this committee will be moving legislation soon to create a stronger, consolidated cybersecurity agency at the Department of Homeland Security. This proposal will elevate the cybersecurity mission at DHS and further enhance cyber operations, including those to more effectively secure Federal networks.

This will help us step up our cyber defense efforts and attract top talent.

And we have already begun to work with DHS and others to make that a reality.

Today, I hope to hear from DHS about how it is working to protect our Federal departments and agencies from these sophisticated cyber threats and what more assistance may be needed. As I'm sure everyone here can agree, we cannot afford another OPM-style breach, we must better ensure our Nation's most sensitive information is protected without any delay.

Mr. RATCLIFFE. Thank you, Chairman.

The Chair now recognizes the Ranking Minority Member of the full committee, the gentleman from Mississippi, Mr. Thompson for his opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I welcome a suite of witnesses here today, and I look forward to their testimony.

Cyber attacks against Federal networks and the Nation have been increasing in frequency in recent years with high-profile breaches of Federal systems at the White House, State Department, Veteran Affairs, and the Office of Personnel Management.

These breaches, many of which are believed to be carried out at the direction of state actors, have called into question the ability

of the Federal Government to adequately secure its data and network.

For instance, there was a massive OPM breach that occurred 2 years ago. In that attack, the personnel records of at least 22 million people were stolen.

These records included very sensitive and personal information about not just Federal employees and contractors, but also about their families and friends. Hackers believed to be working for the Chinese government carried out this malicious attack.

Last week, the committee heard from National security experts about the growing and gathering threat posed by State actors, most notably China, Iran, North Korea, and Russia.

I was struck, however, by the testimony of Dr. Frank Cilluffo, from the George Washington University, who characterized the threats posed by these countries in the following way. "Russia is the most capable. China is very active in computer network export or espionage activity. And North Korea and Iran are the most likely to turn to computer networks attacks to damage our systems."

With respect to Russia, the threat posed by Vladimir Putin has become a kitchen table topic. Americans want to know more about the cyber hacking and influence operation that Putin directed against our democracy in the lead-up to the 2016 elections.

They also want to know if there are any collusion between U.S. person and Russian operatives, to carry out what FBI Director James Comey has called a "successful operation."

These are not minor or trivial concerns. The Russians, as Director Comey has determined, are proud to have sown doubt about the nature of our democratic process and because they were successful, he warned that they will be back.

Mr. Chairman, I was pleased to hear you acknowledge at last week's hearing, that these actions by Russia were an invasion of the privacy of citizens and that they undermined our democratic institution and elections.

Given that the House Intelligence Committee's bipartisan inquiry seems to be unraveling at the hands of its Chairman, now is the time for Members of Congress, regardless of party, to stand together in support of a nonpartisan commission, one akin to the 9/11 Commission.

Turning back to the witnesses before us today, I look forward to hearing from the panel on how DHS is progressing in its Federal cybersecurity role and what more can be done within DHS and across the Federal Government to better mitigate, respond to, and recover from attacks on Federal information systems.

With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 28, 2017

Cyber attacks against Federal networks and the Nation have been increasing in frequency in recent years, with high-profile breaches of Federal systems at the White House, State Department, Veterans Affairs, and the Office of Personnel Management (OPM).

These breaches, many of which are believed to be carried out at the direction of state actors, have called into question the ability of the Federal Government to adequately secure its data and networks.

For instance, there was the massive OPM breach that occurred 2 years ago. In that attack, the personnel records of at least 22 million people were stolen. These records included very sensitive and personal information about not just Federal employees and contractors but also about their families and friends. Hackers believed to be working for the Chinese government carried out this malicious attack.

Last week, the committee heard from National security experts about the growing and gathering threat posed by state actors—most notably China, Iran, North Korea, and Russia. I was struck by the testimony of Dr. Frank Cilluffo from the George Washington University who characterized the threats posed by these countries in the following way—"Russia is the most capable, China is very active in computer network exploit or espionage activity," and North Korea and Iran are the most likely "to turn to computer network attacks" to damage our systems.

With respect to Russia, the threat posed by Vladmir Putin has become a "kitchen table" topic. Americans want to know more about the cyber hacking and influence operation that Putin directed against our democracy in the lead up to the 2016 election.

They also want to know if there was any collusion between U.S. persons and Russian operatives to carry out what FBI Director James Comey has called a "successful" operation. These are not minor or trivial concerns. The Russians, as Director Comey has determined, are proud to have "sowed doubt about the nature of our democratic process" and because they were successful, he warned that "they'll be back."

Mr. Chairman, I was pleased to hear you acknowledge at last week's hearing that these actions by Russia were an invasion of the privacy of citizens and that they undermined our democratic institutions and elections.

Given that the House Intelligence Committee's bipartisan inquiry seems to be unraveling at the hands of its Chairman, now is the time for Members of Congress—regardless of party—to stand together in support of a non-partisan commission, one akin to the 9/11 commission.

Turning back to the witnesses before us today, I look forward to hearing from the panel on how DHS is progressing in its Federal cybersecurity role and what more can be done within DHS and across the Federal Government to better mitigate, respond to, and recover from attacks on Federal information systems.

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

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

MARCH 28, 2017

Chairman Ratcliffe and Ranking Member Richmond, thank you for convening this opportunity for the Homeland Security Committee Subcommittee on Cybersecurity & Infrastructure Protection to review "The Current State of DHS's Efforts to Secure Federal Networks."

Today's hearing will give Members of the Committee an opportunity to hear from individuals inside of the Department of Homeland Security (DHS), the Government Accountability Office; the Congressional Research Service.

I thank today's witnesses:

- Jeanette Manfra, Deputy Under Secretary for Cybersecurity and Communications (Acting), National Programs & Protection Directorate, Department of Homeland Security;
- Gregory Wilshusen, Director, Information Security Issues, Government Accountability Office; and
- Chris Jaikaran, Cybersecurity Analyst, Congressional Research Service (Democratic Witness).

Today's hearing will also give Members an opportunity learn more about DHS's work to create a common security baseline across Federal civilian agencies.

This hearing will also provide an update on the operating an intrusion prevention and detection service known as EINSTEIN, which is designed to insulate Federal networks from attacks and gather threat intelligence.

In the first few weeks of this Congress, I introduced a number of measures on the topic of cybersecurity to address gaps in our Nation's cyber defensive posture:

- CAPITALS Act—H.R. 54—legislation seeking a report on the feasibility of developing a DHS Civilian Cyber Defense National Resource to protect our Nation's critical infrastructure in the event of a terrorist cyber attack;

- SCOUTS Act—H.R. 940—a bill to secure public utilities from terrorist threats;
- SAFETI Act—H.R. 950—directs the Secretary of DHS to provide a report on the agency's response to the Russian attack against our Nation's election system;
- Terrorism Prevention and Critical Infrastructure—H.R. 945; and
- The Cybersecurity and Federal Workforce Enhancement Act—H.R. 935.

CAPITALS Act—H.R. 54, directs that the Department of Homeland Security (DHS) must report to Congress regarding the feasibility of establishing a DHS Civilian Cyber Defense National Resource.

The report provided by the CAPITALS Act will address:

- the number of persons who would be needed to defend the critical infrastructure of the United States from a cyber attack or man-made intentional or unintentional catastrophic incident;
- elements of DHS that would be best equipped to recruit, train, and manage such a resource;
- resources that could be pre-positioned and training that could be instilled to assure responsiveness if an incident disrupts communications in a region or area;
- the impact of potential recruits' lack of experience in military, intelligence, law enforcement, or Government work experience;
- logistics of allowing Governors to make requests of DHS to use such a resource in States during times of cyber emergency; and
- whether a resource trained to defend U.S. networks in a major attack or natural or man-made disaster will benefit overall efforts to defend the interests of the United States.

H.R. 940, the "Securing Communications of Utilities from Terrorist Threats" or the "SCOUTS Act," directs the Secretary of Homeland Security, in coordination with the sector-specific agencies, to work with critical infrastructure owners and operators and State, local, Tribal, and territorial entities to seek voluntary participation in a dialogue with DHS on how the agency can best assist Critical Infrastructure's defense against and recover from terrorist attacks.

H.R. 950, requires a report and assessment regarding Department of Homeland Security's response to terrorist threats to Federal elections. The Comptroller General of the United States is directed to conduct an assessment of the effectiveness of Department of Homeland Security actions to protect election systems from cyber attacks and to make recommendations for improvements to the actions taken by DHS if determined appropriate.

H.R. 935, The "Cybersecurity and Federal Workforce Enhancement Act" identifies and trains people already in the workforce who can obtain the skills to address our Nation's deficit in the number of workers and positions available for those with needed skills.

On June 4, 2015, Office of Personnel Management announced that it would be notifying over 4 million current and former Federal employees of a data breach thought to be committed by Chinese hackers.

OPM officials said that the hacking exposed employee's job assignments, performance, and training.

It was later disclosed that the hackers also gained access to "background or clearance investigations" data.

In February 2016, it was reported in the *Hill* that personal information on 9,000 DHS employees was published on-line.

The information posted on the internet includes names, job titles, email addresses, and phone numbers of employees.

The hacker said they obtained the data by "compromising the email account" of an employee in the Department of Justice.

The security of civil agency networks should be of the greatest concern following what we know was an extensive intrusion into public, and private computing networks last year in Russia's efforts to undermine our Nation's democratic process.

In 2016, it was reported that the Election Assistance Commission, the agency responsible for certifying the security of voting machines reportedly fell victim to what is believed to have been a Russian hacker.

The Security firm "Recorded Future" reported that it discovered EAC employees' computer access information for sale on the internet black market.

In February 2016, the IRS revealed it discovered and stopped an automated cyber attack on its e-filing personal identification number (PIN) system.

The IRS reported that cyber criminals used information stolen from another source to generate 101,000 e-file PINs from taxpayers' stolen Social Security numbers (SSNs).

E-file PINs are used by some taxpayers to electronically file their tax returns—it is worth noting the difficulty the IRS has seen in the past with thieves filing taxes and receiving tax payments due to taxpayers.

The number and severity of data breaches has only grown over the last few years. We can and we must do better at protecting civilian agencies and their data assets from compromise.

I am pleased at the progress being made with Majority and Minority committee staff, along with my staff in finalizing the Prevent Zero Day Events Act, which I plan to introduce.

The Prevent Zero Day Events Act will help DHS in working with Federal agencies in developing strategies for detecting Zero Day events, which are software or firmware vulnerabilities that have gone undetected, but if exploited by a terrorist, would posed a significant threat to the ability of agencies to function.

I look forward to your testimony and the testimony of the second panel for today's hearing.

Thank you.

Mr. RATCLIFFE. We are pleased to have a very distinguished panel of witnesses before us today on this most important topic.

Ms. Jeanette Manfra is the acting deputy under secretary for cybersecurity in the Department of Homeland Security. Welcome.

Mr. Greg Wilshusen is the director for information security issues for the U.S. Government Accountability Office. Good to see you again, Mr. Wilshusen.

Mr. Chris Jaikaran is an analyst for the cybersecurity policy for the Congressional Research Service. Welcome.

I would now ask all of you to stand and raise your right hand so I can swear you in to testify.

[Witnesses sworn.]

Let the record reflect that each witness has answered in the affirmative. You may be seated. The witnesses' full written statements will appear in the record.

The Chair now recognizes Ms. Manfra for 5 minutes for her opening statement.

STATEMENT OF JEANETTE MANFRA, ACTING DEPUTY UNDER SECRETARY FOR CYBERSECURITY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, sir. Chairman Ratcliffe, Ranking Member Richmond, Chairman McCaul, Ranking Member Thompson, and Members of the committee, thank you for today's opportunity to discuss DHS's efforts to secure Federal networks.

Cybersecurity remains one of the most significant risks facing the United States. Working with Congress, we have focused on a range of actions to confront this evolving challenge.

By law, Federal agencies have responsibility for their own cybersecurity. Our goal is to protect agencies against cybersecurity incidents and to help each agency effectively safeguard their own systems and networks.

We achieve these goals in four ways: No. 1, by providing a baseline of security for civilian agencies through the National Cybersecurity Protection System, or NCPS, and the Continuous Diagnostics and Mitigation Program; No. 2, by conducting risk assessments and directing agency action as needed; No. 3, by serving as an information-sharing hub; and No. 4, by providing incident response assistance.

Our first focus area is identifying, prioritizing, and enabling mitigation of cybersecurity threats facing civilian agencies through NCPS, of which EINSTEIN is the principal component.

Recognizing the importance of EINSTEIN, Congress mandated that all civilian agencies fully implement the system, resulting in an increase in EINSTEIN 3 Accelerated coverage from 38 percent to 93 percent over the past year. We are working with the remaining civilian agencies to facilitate full participation.

We recognize that many sophisticated adversaries cannot be blocked by signatures of known threats. NCPS is a platform and EINSTEIN is only a first step. Moving forward, we are pursuing three lines of effort.

First, increasing the number of known cyber threat indicators available. Second, deploying reputation scoring to help Government agencies prioritize specific indicators based upon the likely severity of the treat. Third, piloting an advanced analytics capability to identify anomalous activity that could be a previously-unknown threat.

Effective cybersecurity must address threats. But agencies must also identify and fix known vulnerabilities. Through the Continuous Diagnostics and Mitigation, or CDM program, DHS provides Federal civilian agencies with tools to gain visibility, often for the first time, into the extent of cybersecurity risk across their entire network and prioritize identified issues.

DHS also conducts risk assessments, based upon a standardized methodology and informed by an understanding of relevant threats.

In fiscal year 2017, we are continuing to focus on the most critical systems. DHS leveraged the authority from the Cybersecurity Act of 2015 to issue a binding operational directive, mandating that agencies participate in our high-value asset assessment process and fix identified vulnerabilities within 30 days.

Cybersecurity threats are constantly changing as our adversaries implement new tactics, techniques, and procedures. Recognizing this fact, Congress established our NCCIC as a civilian hub for cyber threat indicators and defensive measures, with Federal and non-Federal entities.

As required by the Cybersecurity Act of 2015, we automated the sharing of our cyber-threat indicators, while protecting privacy and civil liberties.

Persistent adversaries will find ways to infiltrate networks. When an incident occurs, our NCCIC offers assistance to find the adversary, drive them out, restore critical services, and improve security moving forward.

In closing, while we have made progress, we must do more to confront the continually-evolving threats facing our Nation. This commitment to do more is at the core of the pending DHS cybersecurity strategy. This administration is committed to making significant investments in cybersecurity and modernizing our Federal IT infrastructure.

In the fiscal year 2018 budget blueprint, the President requested $1.5 billion for DHS to safeguard cyber space. The Department views the IT modernization effort as an opportunity to review the current approach to Federal network security and potentially make generational advances in the capabilities we offer.

We must also ensure that DHS is appropriately organized to address cybersecurity threats. We appreciate the Chairman of the committee's leadership in working to reauthorize the Department.

As the committee considers these issues, we are committed to working with Congress to ensure a homeland that is more safe, secure, and resilient.

Thank you for the opportunity to testify, and I look forward to any questions you may have.

[The prepared statement of Ms. Manfra follows:]

PREPARED STATEMENT OF JEANETTE MANFRA

MARCH 28, 2017

INTRODUCTION

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to appear before you today. Cybersecurity remains one of the most significant strategic risks to the United States. The past several years have seen a steady drumbeat of cybersecurity compromises affecting the Federal Government, State and local governments, and the private sector. Working with Congress, we have focused on a range of actions to confront this evolving challenge. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-Government incident response capabilities, enhance sharing of information on best practices and cyber threats, and strengthen resilience. The Department of Homeland Security (DHS), through the National Protection and Programs Directorate (NPPD), leads the Federal Government's efforts to secure our Nation's critical infrastructure and protect Federal civilian networks from malicious cyber activity.

Over the past few years, the Federal Government has made significant progress in improving agency cybersecurity, establishing a common baseline of protection, and codifying roles and responsibilities to effectively manage cybersecurity risks and incidents. Through engagements with State, local, Tribal, and territorial (SLLT) governments, and the private sector, we have provided technical assistance upon request and expanded information-sharing capabilities to improve situational awareness of threats, vulnerabilities, incidents, mitigation, and recovery actions. Today, I will discuss the roles of NPPD in protecting the Federal civilian Executive branch networks.

Under the *Federal Information Security Modernization Act of 2014 (FISMA),* agencies have primary responsibility for their own cybersecurity, the Office of Management and Budget (OMB) generally develops and oversees agency implementation of information security policies and practices, and DHS administers the implementation of those policies and practices. As part of securing their own systems, agencies must comply with OMB policies, DHS directives, and National Institute of Standards and Technology (NIST) standards and guidelines. DHS, pursuant to its various authorities, provides a common set of security tools across the civilian Executive branch and helps agencies manage their cyber risk. NPPD's assistance to agencies includes: (1) Providing tools to safeguard civilian Executive branch networks through the National Cybersecurity Protection System (NCPS), which includes EINSTEIN, and Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. DHS's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination.

EINSTEIN

EINSTEIN refers to the suite of intrusion detection and prevention capabilities that protects agencies' Unclassified networks at the perimeter of each agency. EINSTEIN provides situational awareness of civilian Executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

The first two phases of EINSTEIN—EINSTEIN 1 and 2—allow DHS to identify potentially malicious activity and to conduct critical analysis after an incident occurs, as well as to detect known malicious traffic. In 2015, DHS estimated these ca-

pabilities screened over 90 percent of all Federal civilian internet traffic. On a typical day, EINSTEIN 2 intrusion detection sensors generate approximately 30,000 alerts about potential malicious cyber activity. These alerts are evaluated by DHS cybersecurity analysts to determine whether the alert represents an active threat and potential compromise, and if further mitigation or remediation is needed.

EINSTEIN 3 Accelerated (EINSTEIN 3A) is the intrusion prevention capability, which blocks known malicious traffic. Intrusion prevention is provided as a service by internet service providers (ISPs) serving the Federal Government. The initial implementation of EINSTEIN 3A involves two intrusion prevention security services by the ISPs: domain name server (DNS) sinkholing and email filtering. DHS is working with the ISPs to add further protections. EINSTEIN 1 and 2 use only Unclassified cyber threat indicators, while EINSTEIN 3A uses Unclassified and Classified indicators. These signature-based capabilities use indicators of compromise to detect and block known malicious traffic.

In the Cybersecurity Act of 2015, Congress directed each Executive branch civilian agency to apply available EINSTEIN protections to all information traveling to or from an agency information system by December 18, 2016. Agencies have made significant progress in implementing available EINSTEIN protections. Prior to passage of the Act, EINSTEIN 3A covered approximately 38 percent of Federal civilian users. Today, EINSTEIN 3A is protecting a significant percentage of the Executive branch civilian workforce at the 23 largest agencies and most agencies have at least one of its two intrusion prevention capabilities. DHS continues to work with all remaining Federal civilian agencies to facilitate their full participation in EINSTEIN. At the same time, our NCPS program is also developing new capabilities and conducting a strategic review of the program architecture that will provide even more protections for Federal agencies.

Today, EINSTEIN is a signature-based intrusion detection and prevention capability that takes action on known malicious activity. Leveraging existing investments in the ISP infrastructure, our non-signature-based pilot efforts to move beyond current reliance on signatures are yielding positive results in the discovery of previously-unidentified malicious activity. DHS is demonstrating the ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, Government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as the skill sets and personnel required to operationalize the non-signature based approach to cybersecurity.

SLTT governments are able to access intrusion detection and analysis services through the Multi-State Information Sharing and Analysis Center (MS–ISAC). MS–ISAC's service, called Albert, closely resembles EINSTEIN 2. While the current version of Albert cannot actively block known cyber threats, it can alert cybersecurity officials to an issue for further investigation. DHS worked closely with MS–ISAC to develop the program and considers MS–ISAC to be the principal conduit for sharing cybersecurity information with State governments.

Continuous Diagnostics and Mitigation (CDM)

EINSTEIN, our tool to address perimeter security will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. CDM provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common Federal dashboard. CDM is divided into four phases:

- CDM Phase 1 identifies all computers and software on agency networks and checks for known vulnerabilities.
- CDM Phase 2 allows agencies to better manage identities, accounts, and privileges for the people and services using their networks.
- CDM Phase 3 will assess activity happening on agencies' networks to identify anomalies and alert security personnel.
- CDM Phase 4 will protect sensitive and high-value data within agency networks.

Significant progress has been made in the deployment of CDM. DHS has assessed the needs of the Executive branch civilian agencies and has completed the purchasing of most CDM Phase 1 tools. Agencies are now installing the tools across their networks, including six agencies that have fully deployed all Phase 1 tools as well as the agency dashboards, which give network administrators visibility into the current state of their networks to better identify and prioritize areas of cyber risk. DHS has also awarded two CDM Phase 2 contracts, focusing on strong authentica-

tion for administrative users as well as general users, making the associated tools available to all participating agencies.

This summer, CDM will begin supplementing the existing CDM agency dashboards by introducing the Federal CDM Dashboard, which will provide the National Cybersecurity and Communications Integration Center (NCCIC) with greater insight into the Federal enterprise cybersecurity posture. The summary data available at the Federal level presents a view of the relative risk and network health across the Federal Government to inform policy decisions and operational guidance, provide timely reporting for addressing critical issues affecting multiple agencies, and enable cost-effective and efficient FISMA reporting.

CDM will help us achieve two major advances for Federal cybersecurity. First, agencies will have visibility, often for the first time, into the extent of cybersecurity risks across their entire network and gain the ability to prioritize identified issues based upon their relative importance. Second, the NCCIC will be able to identify systemic risks across the civilian Executive branch. An example is illustrative. Currently, when a vendor announces a major vulnerability, the NCCIC tracks Government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will allow the NCCIC to immediately view the prevalence of a given device or software type across the Federal Government so that the NCCIC can provide agencies with timely guidance on their risk exposure. Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian Executive branch.

CDM tools are currently available through blanket purchase agreement negotiated by the General Services Administration on DHS's behalf. This agreement leverages the Government-wide volume to provide the best value and cost savings to the Federal Government. For example, by grouping agency requirements in Phases 1 and 2, we have saved the Federal Government millions of dollars on product purchases. Many SLTT governments are also able to purchase tools from this purchase agreement. By purchasing commercial CDM tools, SLTT governments can take advantage of bulk purchasing cost savings and invest those savings in their own cybersecurity resilience.

Measuring and Motivating Agencies to Improve Cybersecurity

DHS conducts a number of activities to measure agencies' cybersecurity practices and work with agencies to improve risk management practices.

The Cybersecurity Framework, is voluntary guidance, based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk and was developed by NIST through collaboration with diverse parts of industry, academia, and Government, including DHS. DHS promotes the use of NIST standards, guidelines, minimum information security requirements, including the Cybersecurity Framework.

FISMA provided the Secretary of Homeland Security with the authority to develop and oversee implementation of binding operational directives to agencies. In 2016, the Secretary issued a binding operational directive on securing high-value assets (HVA), or those assets, Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' National security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. DHS works with several interagency partners to prioritize HVAs for assessment and remediation activities across the Federal Government. For instance, DHS conducts security architecture reviews on these HVAs to help agencies assess their network architecture and configurations.

As part of the effort to secure HVAs, DHS conducts in-depth vulnerability assessments of prioritized agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these assessments on Federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private sector and SLTT partners. DHS also works with GSA to ensure our industry partners can provide assessments that align with our HVA initiative to agencies, if necessary.

Another binding operational directive issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing devices.

The NCCIC conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's binding operational directive and have sustained this progress. When the Secretary issued this directive, NPPD identified over 360 "stale" critical vulnerabilities across Federal civilian agencies. By "stale" I mean the vulnerabilities had been known for at least 30 days and were still not patched. Since December 2015, DHS has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified.

By conducting vulnerability assessments and security architecture reviews, DHS is helping agencies find and fix vulnerabilities, and secure their networks before an incident occurs.

Information Sharing

By sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from other partners helps us understand emerging risks and develop effective protective measures.

Congress authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among Federal and non-Federal entities, including the private sector. As required by the Cybersecurity Act of 2015, we established a capability, known as Automated Indicator Sharing (AIS), to automate our sharing of cyber threat indicators in real-time. AIS protects the privacy and civil liberties of individuals by narrowly tailoring the information shared to that which is necessary to characterize identified cyber threats, consistent with long-standing DHS policy and the requirements of the Act. AIS is a part of the Department's effort to create an ecosystem in which as soon as a company or Federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing limits the scalability of any attack techniques, which increases the costs for adversaries and should reduce the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense should enable organizations to enhance their defenses against the most common cyber attacks, freeing their cybersecurity staff to concentrate on the novel and sophisticated attacks. Over 129 agencies and private-sector partners have connected to DHS's AIS capability. Notably, partners such as information sharing and analysis organizations (ISAOs) and computer emergency response teams further share with or protect their customers and stakeholders, significantly expanding the impact of this capability. AIS is still a new capability and we expect the volume of threat indicators shared through this system to substantially increase as the technical standards, software, and hardware supporting the system continue to be refined and put into full production. As more indictors are shared from other Federal agencies, SLTT governments, and the private sector, this information-sharing environment will become more robust and effective.

Another part of the Department's overall information-sharing effort is to provide Federal network defenders with the necessary context regarding cyber threats to prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis (I&A) is continuously assessing the specific threats to Federal networks using traditional all source methods and indicators of malicious activity observed by NCCIC sensors so that the NCCIC can share with Federal network defenders in collaboration with I&A. I&A personnel sit on the NCCIC watch floor.

Incident Response

Cybersecurity is about risk management, and we cannot eliminate all risk. Partners that implement best practices and share information will increase the cost for malicious actors and stop many threats. But ultimately, persistent adversaries will find ways to infiltrate networks in both Government and the private sector. In fiscal year 2016, the NCCIC received reports of 30,899 impactful incidents across the eight attack vectors at Federal agencies, according to the FISMA Annual Report to Congress. When an incident does occur, the NCCIC offers assistance upon request to find the adversary, drive them out, and restore service.

CONCLUSION

At all levels, the Federal Government continues to be targeted by a wide range of malicious cyber actors attempting to gain access to sensitive systems. We have made significant progress over the past year: We have provided a baseline of CDM Phase 1 tools, we have expanded the coverage of EINSTEIN 3A, we have expanded risk and vulnerability assessments, we have operationalized the automated indi-

cator-sharing capability, and we have established a useful architecture for coordinating the Federal Government's response to significant cyber incidents. But there is more to be done. This administration will make significant investments in cybersecurity. In the recently-released budget blueprint, the President requested $1.5 billion for DHS to safeguard cyber space by protecting Federal networks and critical infrastructure from an attack. Through a suite of advanced cybersecurity tools and more assertive defense of Government networks, NPPD would share more cybersecurity incident information with other Federal agencies and the private sector, leading to faster responses to cybersecurity attacks.

We must also ensure that DHS is appropriately organized to address today's and tomorrow's cybersecurity threats, and we appreciate the Chairman of the Committee's leadership in working to reauthorize the Department. As the committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that ensures a homeland that is more safe, secure, and resilient.

Mr. RATCLIFFE. Thank you, Ms. Manfra.

The Chair now recognizes Mr. Wilshusen for 5 minutes for his opening statement.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Ratcliffe, Ranking Member Richmond, Ranking Member Thompson, and Members of the subcommittee, thank you for the opportunity to discuss DHS's efforts to secure Federal computer networks. As recent cyber attacks have illustrated, the need for robust and effective cybersecurity has never been greater.

Today, I will focus on two of the Department's programs: The National Cybersecurity Protection System, also known as EINSTEIN, which is an intrusion detection and prevention system, and the Continuous Diagnostics and Mitigation Program.

But before I do, if I may, I would like to recognize members of my team who were instrumental in developing my statement and performing the work under PENIA. With me today is Mike Gilmore and Kush Malhotra. In addition, Jeff Knott, Angela Watson, Nancy Glover, and Scott Pettis also made significant contributions to the work.

Mr. Chairman, as you know, several Federal laws establish key Government-wide roles for DHS with securing Federal information systems. Consistent with these laws, DHS is leading the EINSTEIN and CDM programs to assist Federal agencies in protecting their computer networks and systems. Our work has highlighted the need for advances with these programs.

In January 2016, we reported that EINSTEIN was limited in its ability to detect malicious network activity because it could only match against known patterns of malicious data or signatures.

It was unable to detect intrusions for which it did not have a valid or enabled signature deployed because it did not provide for anomaly-based intrusion detection capability. Such a capability involves comparing current network activity against pre-defined baselines of normal network behavior to identify deviations which could indicate malicious activity.

EINSTEIN was also unable to detect exploits across all types of network traffic because it was not monitoring or had not deployed signatures related to certain types of network traffic. As a result,

it would not have detected known malicious data embedded in such traffic.

In addition, DHS's process for notifying agencies of detected malicious activity was not always effective, with disagreement among DHS and the five agencies we reviewed about the number of incident notifications sent and received and their usefulness.

We made nine recommendations to DHS for expanding or enhancing EINSTEIN's capabilities, including those for detecting and preventing malicious traffic, notifying agencies of potential incidents, and developing guidance for routing network traffic through EINSTEIN's sensors. The Department concurred with each of our recommendations and has stated that it has taken or is taking actions to implement them.

The tools and services delivered through DHS's CDM program are intended to provide agencies with the capability to automate network monitoring, correlate and analyze security-relevant information, and enhanced risk-based decision making at both the agency and Government-wide levels.

In May 2016, GAO reported that most of the 17 agencies we surveyed responded that they were in the early stages of CDM implementation. For example, 14 agencies reported that they had deployed products to monitor or scan hardware and software inventories, configuration settings, and common vulnerabilities. But only two had completed installation of dashboards at the agency or component level.

We believe that the use of tools and of capabilities available under the CDM program, if effectively implemented by agencies, can help them to identify and resolve cybersecurity vulnerabilities in a prioritized and risk-based manner.

In conclusion, EINSTEIN and CDM offer the prospect of important advances in the security over Federal systems. Enhancing EINSTEIN's capabilities and greater adoption by agencies will help DHS achieve the full benefit of the system.

An effective implementation of CDM functionality by Federal agencies could better position them to protect their information technology resources from evolving and pernicious threats.

Chairman Ratcliffe, Ranking Member Richmond, and Ranking Member Thompson, Members of the subcommittee, this concludes my statement. I would be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

MARCH 28, 2017

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee: Thank you for the opportunity to appear before you to discuss the Department of Homeland Security's (DHS) efforts to secure Federal computer networks. As recent cyber attacks have illustrated, the need for robust and effective cybersecurity has never been greater.

Today, I will provide an overview of our work related to efforts by DHS to improve the cybersecurity posture of the Federal Government. In particular, I will focus on two of the Department's initiatives: The National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN, and the Continuous Diagnostics and Mitigation (CDM) program.

In developing this testimony, we relied on our previous reports [1] as well as information provided by the Department on its actions in response to our previous recommendations. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

The work on which this statement is based was conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate 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

Federal agencies are dependent on computerized (cyber) information 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 the Nation's safety, prosperity, and well-being. Virtually all Federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective security controls to protect these systems and data could have a significant impact on a broad array of Government operations and assets.

Computer networks and systems used by Federal agencies are often riddled with security vulnerabilities—both known and unknown. These systems are often interconnected with other internal and external systems and networks, including the internet, thereby increasing the number of avenues of attack and expanding their attack surface.

In addition, cyber threats to systems supporting the Federal Government are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, foreign nations—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Safeguarding Federal computer systems has been a long-standing concern. This year marks the 20th anniversary of when GAO first designated information security as a Government-wide high-risk area in 1997.[2] We expanded this high-risk area to include safeguarding the systems supporting our Nation's critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.[3]

Over the last several years, GAO has made about 2,500 recommendations to agencies aimed at improving the security of Federal systems and information. These recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. Many agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. As of February 2017, about 1,000 of our information security-related recommendations had not been implemented.

Our audits of the effectiveness of information security programs and controls at Federal agencies have consistently shown that agencies are challenged in securing

---

[1] GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO–16–294 (Washington, DC: Jan. 28, 2016); *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO–16–501 (Washington, DC: May 18, 2016); *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk*, GAO–16–513 (Washington, DC: Aug. 30, 2016); *Information Security: Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data*, GAO–16–493 (Washington, DC: Apr. 28, 2016); *Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data*, GAO–16–398 (Washington, DC: Mar. 28, 2016); *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls*, GAO–16–265 (Washington, DC: Mar. 23, 2016); *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO–15–714 (Washington, DC: Sept. 29, 2015); *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO–15–221 (Washington, DC: Jan. 29, 2015); and *Information Security: VA Needs to Address Identified Vulnerabilities*, GAO–15–117 (Washington, DC: Nov. 13, 2014).

[2] GAO designates agencies and program areas as high-risk due to their vulnerability to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

[3] See GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO–17–317 (Washington, DC: Feb. 15, 2017).

their information systems and information. In particular, agencies have been challenged in the following activities:

- *Enhancing capabilities to effectively identify cyber threats to agency systems and information*.—A key activity for assessing cybersecurity risk and selecting appropriate mitigating controls is the identification of cyber threats to computer networks, systems, and information. In 2016, we reported on several factors that agencies identified as impairing their ability to identify these threats to a great or moderate extent. The impairments included an inability to recruit and retain personnel with the appropriate skills, rapidly-changing threats, continuous changes in technology, and a lack of Government-wide information-sharing mechanisms.[4] We believe that addressing these impairments will enhance the ability of agencies to identify the threats to their systems and information and be in a better position to select and implement appropriate countermeasures.
- *Implementing sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices*.—In our reports, we routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment. We believe that establishing strong configuration standards and implementing sustainable processes for monitoring and enabling configuration settings will strengthen the security posture of Federal agencies.
- *Patching vulnerable systems and replacing unsupported software*.—Federal agencies we have reviewed consistently fail to apply critical security patches on their systems in a timely manner, sometimes doing so years after the patch becomes available. We have consistently identified instances where agencies use software that is no longer supported by their vendors. These shortcomings place agency systems and information at significant risk of compromise, since many successful cyber attacks exploit known vulnerabilities associated with software products. We believe that using vendor-supported and patched software will help to reduce this risk.
- *Developing comprehensive security test and evaluation procedures and conducting examinations on a regular and recurring basis*.—Federal agencies we have reviewed often do not test or evaluate their information security controls in a comprehensive manner. The agency evaluations we reviewed were sometimes based on interviews and document reviews (rather than in-depth security evaluations), were limited in scope, and did not identify many of the security vulnerabilities that our examinations identified. We believe that conducting in-depth security evaluations that examine the effectiveness of security processes and technical controls is essential for effectively identifying system vulnerabilities that place agency systems and information at risk.

Federal Laws Provide a Framework for Securing Agencies' Information and Systems

The Federal Information Security Modernization Act of 2014 (FISMA)[5] provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and for ensuring the effective oversight of information security risks, including those throughout civilian, National security, and law enforcement agencies. The law requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency.

FISMA also establishes key Government-wide roles for DHS. Specifically, with certain exceptions, DHS is to administer the implementation of agency information security policies and practices for information systems including:

- monitoring agency implementation of information security policies and practices;
- providing operational and technical guidance to agencies;
- operating a central Federal information security incident center; and
- deploying technology upon request to assist the agency to continuously diagnose and mitigate cyber threats and vulnerabilities.

---

[4] GAO, *Information Security: Agencies Need to Improve Controls Over Selected High-Impact Systems,* GAO–16–501 (Washington, DC: May 18, 2016).

[5] The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113–283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III of the E-Government Act of 2002 (Pub. L. No. 107–347, Dec. 17, 2002). As used here, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

In addition, the Cybersecurity Act of 2015 requires DHS to deploy, operate, and maintain for use by any Federal agency, a capability to: (1) Detect cybersecurity risks in network traffic transiting to or from agency information systems and (2) prevent network traffic with such risks from traveling to or from an agency information system or modify the traffic to remove the cybersecurity risk.[6]

ADVANCING DHS INITIATIVES COULD IMPROVE THE CYBERSECURITY POSTURE OF THE FEDERAL GOVERNMENT

In implementing Federal law for securing agencies' information and systems, DHS is spearheading several initiatives to assist Federal agencies in protecting their computer networks and electronic information. These include NCPS, CDM, and other services. However, our work has highlighted the need for advances within these initiatives.

NCPS Capabilities and Adoption Could Be Improved

Operated by DHS's United States Computer Emergency Readiness Team (US–CERT),[7] NCPS is intended to detect and prevent cyber intrusions into agency networks, analyze network data for trends and anomalous data, and share information with agencies on cyber threats and incidents. Deployed in stages, NCPS, operationally known as EINSTEIN, has provided increasing capabilities to detect and prevent potential cyber attacks involving the network traffic entering or exiting the networks of participating Federal agencies. Table 1 provides an overview of the EINSTEIN deployment stages to date.

TABLE 1.—OVERVIEW OF THE NATIONAL CYBERSECURITY PROTECTION SYSTEM (NCPS) DEPLOYMENT

Operational Name	Deployment Year	NCPS Objective	Description
EINSTEIN 1	2003	Intrusion detection.	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their internet connections.[1]
EINSTEIN 2	2009	Intrusion detection.	Monitors Federal agency internet connections for specific predefined signatures of known malicious activity and alerts US–CERT when specific network activity matching the predetermined signatures is detected.[2]
EINSTEIN 3 ..... Accelerated	2013	Intrusion detection. Intrusion prevention.	Automatically blocks malicious traffic from entering or leaving Federal civilian agency networks. This capability is managed by internet service providers, who administer intrusion prevention and threat-based decision making using DHS-developed indicators of malicious cyber activity to develop signatures.[3]

Source: GAO analysis of Department of Homeland Security data. GAO–17–518T

[1] The network traffic information includes source and destination internet protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[6] Div. N, sec. 223, Pub. L. No. 114–113 (Dec. 18, 2015); 129 Stat. 2935, 2964; 6 U.S.C. § 151.

[7] Within DHS, US–CERT is a component of the National Cybersecurity and Communications Integration Center. It serves as the central Federal information security incident center specified by FISMA.

[2] Signatures are recognizable, distinguishing patterns associated with cyber attacks, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

[3] An indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data may be related to internet protocol addresses, domains, e-mail headers, files, and character strings. Indicators can be either Classified or Unclassified.

The overarching objectives of NCPS are to provide functionality that supports intrusion detection, intrusion prevention, analytics, and information sharing.[8] However, in January 2016, we reported that NCPS had partially, but not fully, met these objectives:[9]

- *Intrusion detection*.—NCPS provided DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at Federal agencies. Specifically, NCPS compared network traffic to known patterns of malicious data, or "signatures," but did not detect deviations from pre-defined baselines of normal network behavior. In addition, NCPS did not monitor several types of network traffic and therefore would not have detected malicious traffic embedded in such traffic. NCPS also did not examine traffic for certain common vulnerabilities and exposures that cyber threat adversaries could have attempted to exploit during intrusion attempts.
- *Intrusion prevention*.—The capability of NCPS to prevent intrusions was limited to the types of network traffic it monitored. For example, the intrusion prevention function monitored and blocked e-mail determined to be malicious. However, it did not monitor malicious content within web traffic, although DHS planned to deliver this capability in 2016.
- *Analytics*.—NCPS supported a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. However, DHS had not developed planned capabilities to facilitate near real-time analysis of various data streams, perform advanced malware behavioral analysis, and conduct forensic analysis in a more collaborative way. DHS planned to develop and implement these enhancements through 2018.
- *Information sharing*.—DHS had yet to develop most of the planned functionality for NCPS's information-sharing capability, and requirements had only recently been approved at the time of our review. Agencies and DHS also did not always agree about whether notifications of potentially malicious activity had been sent or received, and agencies had mixed views about the usefulness of these notifications. Further, DHS did not always solicit—and agencies did not always provide—feedback on them.

In addition, while DHS had developed metrics for measuring the performance of NCPS, the metrics did not gauge the quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities. As a result, DHS was unable to describe the value provided by NCPS.

To enhance the functionality of NCPS, we made six recommendations to DHS, which if implemented, could help the agency to expand the capability of NCPS to detect cyber intrusions, notify customers of potential incidents, and track the quality, efficiency, and accuracy of supporting actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information. DHS concurred with the recommendations. In February 2017 when we followed up on the status of the recommendations, DHS officials stated that they have implemented 2 of the recommendations and initiated actions to address the other 4 recommendations. We are in the process of evaluating DHS's actions for the two implemented recommendations.

In January 2016, we also reported that Federal agencies had adopted NCPS to varying degrees. Specifically, the 23 civilian agencies covered by the *Chief Financial Officers (CFO) Act*[10] that were required to implement the intrusion detection capabilities had routed some traffic to NCPS intrusion detection sensors. However, as of January 2016, only 5 of the 23 agencies were receiving intrusion prevention services, due to certain policy and implementation challenges. For example, officials

[8] The National Institute of Standards and Technology (NIST) describes intrusion detection as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to bypass the security mechanisms of a computer or network or to compromise the confidentiality, integrity, and availability of the information they contain. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Analytics is the synthesis of knowledge from the collection, preparation, and analysis of data. Information sharing is the process of exchanging of cyber threat and incident data.

[9] GAO–16–294.

[10] 31 U.S.C. 901(b).

stated that the ability to meet DHS security requirements to use the intrusion prevention capabilities varied from agency to agency. Further, agencies had not taken all the technical steps needed to implement the system, such as ensuring that all network traffic was being routed through NCPS sensors. This occurred in part because DHS had not provided network routing guidance to agencies. As a result, it had limited assurance regarding the effectiveness of the system.

We recommended that DHS work with Federal agencies and the internet service providers to document secure routing requirements in order to better ensure the complete, safe, and effective routing of information to NCPS sensors. DHS concurred with the recommendation. When we followed up with DHS on the status of the recommendations, DHS officials said that nearly all of the agencies covered by the CFO Act are receiving at least one of the intrusion prevention services, as of March 2017. Further, the officials stated that DHS has collaborated with the Office of Management and Budget (OMB) to develop new guidance for agencies on perimeter security capabilities as well as alternative routing strategies. We will evaluate the network routing guidance when DHS finalizes and implements it.

Effective Implementation of the CDM Program Could Improve Information Security at Agencies

The CDM program provides Federal agencies with tools and services that are intended to provide them with the capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and Government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed into a dashboard that alerts network managers and enables the agency to allocate resources based on the risk.

DHS, in partnership with and through the General Services Administration, established a Government-wide acquisition vehicle for acquiring continuous diagnostics and mitigation capabilities and tools. The CDM blanket purchase agreement is available to Federal, State, local, and Tribal government entities for acquiring these capabilities.

There are three phases of CDM implementation:

Phase 1.—This phase involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. According to the Cybersecurity Strategy and Implementation Plan, DHS purchased Phase 1 tools and integration services for all participating agencies in fiscal year 2015.

Phase 2.—This phase intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized activity. According to the Cybersecurity Strategy and Implementation Plan, DHS was to provide agencies with additional Phase 2 capabilities throughout fiscal year 2016, with the full suite of CDM phase 2 capabilities delivered by the end of that fiscal year.

Phase 3.—According to DHS, this phase is intended to address boundary protection and event management for managing the security life cycle. It focuses on detecting unusual activity inside agency networks and alerting security personnel. The agency planned to provide 97 percent of Federal agencies the services they need for CDM Phase 3 in fiscal year 2017.

As we reported in May 2016,[11] most of the 18 agencies covered by the CFO Act that had high-impact systems[12] were in the early stages of CDM implementation. All 17 of the civilian agencies[13] that we surveyed indicated they had developed their own strategy for information security continuous monitoring. Additionally, according to survey responses, 14 of the 17 had deployed products to automate hardware and software asset configuration settings and common vulnerability management. Further, more than half of the agencies noted that they had leveraged products/tools

---

[11] GAO, *Information Security: Agencies Need to Improve Controls Over Selected High-Impact Systems*, GAO–16–501 (Washington, DC: May 18, 2016). We surveyed the 18 agencies covered by the Chief Financial Officers (CFO) Act that reported having high-impact systems on a variety of information security-related issues including their implementation of Government-wide security initiatives such as the CDM program.

[12] High-impact systems are those where the loss of the confidentiality, integrity, or availability of the information or information system could be expected to have a severe or catastrophic adverse effect on organizations operations, assets, or personnel. For example, it might cause the organization to be unable to perform one or more of its primary functions or result in a major financial loss. Of the 24 CFO Act agencies, 18 reported having high-impact systems at the time of our review.

[13] The Department of Defense, one of the 18 agencies with high-impact systems, is not required to participate in the CDM program.

provided through the General Services Administration's acquisition vehicle. However, only 2 of the 17 agencies reported that they had completed installation of agency and bureau/component-level dashboards and monitored attributes of authorized users operating in their agency's computing environment. Agencies also noted that expediting the implementation of CDM phases could be of benefit to them in further protecting their high-impact systems.

The effective implementation of the CDM tools and capabilities can assist agencies in overcoming the challenges we have identified that they face when securing their information systems and information. As noted earlier, our audits often identify insecure configurations, unpatched or unsupported software, and other vulnerabilities in agency systems. We believe that the tools and capabilities available under the CDM program, when effectively used by agencies, can help them to diagnose and mitigate vulnerabilities to their systems. By continuing to make these tools and capabilities available to Federal agencies, DHS can also have additional assurance that agencies are better-positioned to protect their information systems and information.

Other DHS Services Are Available to Help Protect Systems, but Are Not Always Used by Agencies

DHS provides other services that could help agencies protect their information systems. Such services include, but are not limited to:

- *US–CERT monthly operational bulletins* are intended to provide senior Federal Government information security officials and staff with actionable information to improve their organization's cybersecurity posture based on incidents observed, reported, or acted on by DHS and US–CERT.
- *CyberStat reviews* are in-depth sessions with National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration. According to OMB, these interviews are face-to-face, evidence-based meetings intended to ensure agencies are accountable for their cybersecurity posture. The sessions are to assist the agencies in developing focused strategies for improving their information security posture in areas where there are challenges.
- *DHS Red and Blue Team exercises* are intended to provide services to agencies for testing their systems with regard to potential attacks. A Red Team emulates a potential adversary's attack or exploitation capabilities against an agency's cybersecurity posture. The Blue Team defends an agency's information systems when the Red Team attacks, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group.

In May 2016, we reported that although participation varied among the 18 agencies we surveyed, most of those that chose to participate generally found these services to be useful in aiding the cybersecurity protection of their high-impact systems.[14] Specifically,

- 15 of 18 agencies participated in US–CERT monthly operational bulletins, and most found the service very or somewhat useful.
- All 18 agencies participated in the CyberStat reviews, and most found the service very or somewhat useful.
- 9 of 18 agencies participated in DHS's Red/Blue team exercises, and most found the exercises to be very or somewhat useful.

Half of the agencies in our survey reported that they wanted an expansion of Federal initiatives and services to help protect their high-impact systems. For example, agencies noted that expediting the implementation of CDM phases, sharing threat intelligence information, and sharing attack vectors, could be of benefit to them in further protecting their high-impact systems. We believe that by continuing to make these services available to agencies, DHS will be better able to assist agencies in strengthening the security of their information systems.

In conclusion, DHS is leading several programs that can benefit Federal efforts to secure agency information systems and information. Two such programs, NCPS and CDM, offer the prospect of important advances in the security over Federal systems. Enhancing NCPS's capabilities and greater adoption by agencies will help DHS achieve the full benefit of the system. Effective implementation of CDM functionality by Federal agencies could better position them to protect their information technology resources from evolving and pernicious threats.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, this concludes my statement. I would be happy to respond to your questions.

---

[14] See GAO–16–501.

Mr. RATCLIFFE. Thank you, Mr. Wilshusen, and thanks to your team members for their work, as you recognized.

The Chair now recognizes Mr. Jaikaran—did I say that right—for 5 minutes for his opening statement.

STATEMENT OF CHRIS A. JAIKARAN, ANALYST, CYBERSECURITY POLICY, CONGRESSIONAL RESEARCH SERVICE, LIBRARY OF CONGRESS

Mr. JAIKARAN. Chairman Ratcliffe, Ranking Member Richmond, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to testify on the current state of DHS's efforts to secure Federal networks. My name is Chris Jaikaran, and I am an analyst in cybersecurity policy at the Congressional Research Service.

In this role, I research and analyze cybersecurity issues and their policy implications. I have provided a written statement and will summarize that testimony with some brief remarks.

My testimony today will address the legislation that Congress recently passed, the roles and responsibilities assigned by those pieces of legislation, and the policy outcomes from those pieces of legislation.

During the 113th and 114th Congresses, three pieces of legislation were enacted to change how Federal network security is managed: The Federal Information Security Modernization Act of 2014, or FISMA, the National Cybersecurity Protection Act of 2014, and the Cybersecurity Act of 2015.

My written testimony briefly summarizes the effect of this group of legislation on Federal network security without addressing other cybersecurity concerns, such as the effects on the private sector.

To take an organizational view, these laws establish certain roles and responsibilities among Federal entities for the security of the dot-gov domain. It may be helpful to think of OMB as the strategic, DHS as the operational, and individual agencies as the tactical.

OMB, exercising its oversight of agency budgets, oversees agency adoption of cybersecurity practices and ensures that agencies adopt a cybersecurity posture commensurate to their risk.

DHS oversees agency adoption of cybersecurity programs, provides tools to protect agency networks, and coordinates Government-wide efforts on Federal cybersecurity.

Individual agencies ensure that risks are effectively managed in their own agency, with cybersecurity being one such risk. In accordance with provisions in FISMA as amended, agency heads shall ensure that the responsibility for cybersecurity is delegated to a senior official, frequently a chief information security officer.

The 113th Congress marked a shift in legislative policy concerning Federal cybersecurity. Prior to the 113th Congress, cybersecurity risks were one of many risks that an agency head was statutorily required to manage. In managing these cybersecurity risks, their collective risk management equated to the security of the dot-gov domain.

DHS, OMB, and NIST provided programs, information, tools, and guidance to assist agencies in managing that risk, to include FISMA guidance and EINSTEIN. However, it was incumbent upon the agency head to accept those tools and implement that guidance.

With the legislation enacted in the 113th and 114th Congresses, Congress further updated the law to reflect that risk exists not just at the agency level, but across the entire Federal Government.

Federal agencies face risk, not just for the information that agency possesses or the work that agency performs, but because that agency is an element of the Federal Government itself.

The clarification of DHS's role in mitigating risk to all Federal civilian agencies is the operationalization of that change.

By consolidating these responsibilities at DHS, the intent is for DHS to monitor risk to the dot-gov domain and to take action to mitigate that risk, to detect malicious activity at one agency and prevent or mitigate that activity at another agency before it can become disruptive, a sort-of herd protection for civilian agencies.

This construct is also intended to free up agency resources to focus on mitigating the unique cybersecurity risks against agency networks and against agency information technology systems. This distinction between Federal enterprise and the agencies' enterprise appears to be continuing in the new administration.

Early indications from the administration officials signal that the position of the administration is to manage risks to the Federal enterprise as a single entity, rather than as distributed risk across all agencies.

Shifting some additional cybersecurity actions from individual agencies to a single entity responsible for the security of all agencies is intended to allow those agencies to focus their resources on executing their respective missions.

Binding operational directives are an example of the policy shift enacted with this group of legislation. These directives are issued by DHS and require an agency to take some action in order to protect the agency's information technology.

This is a unique relationship, wherein one cabinet-level agency can direct another to take action. In this case, expend the agency's resources for the purposes of managing risk to that agency or the Federal Government, but not risk to DHS.

This concludes my brief remarks. Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Jaikaran follows:]

PREPARED STATEMENT OF CHRIS JAIKARAN

MARCH 28, 2017

INTRODUCTION

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to testify on the current state of efforts by the Department of Homeland Security (DHS) to secure Federal networks. My name is Chris Jaikaran and I am an analyst in Cybersecurity Policy at the Congressional Research Service. In this role, I research and analyze cybersecurity issues and their policy implications.

My testimony today will address legislation recently passed by Congress, the roles and responsibilities assigned by those pieces of legislation, and the potential impact of that legislation on Federal network security.

LEGISLATION

During the 113th and the 114th Congresses, three pieces of legislation were enacted that changed how Federal network security is managed. The testimony below briefly summarizes the effect of the legislation on Federal network security without addressing other cybersecurity concerns, such as effects on the private sector.

Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2014 (FISMA) was enacted during the 113th Congress and codified the existing role the Department of Homeland Security (DHS) was already performing securing Federal networks.[1] FISMA authorized DHS to assist OMB in developing and implementing agency information security programs, coordinating with agencies on cybersecurity, and providing assistance to agencies in achieving cybersecurity. The law also authorized DHS to issue binding operational directives, which are discussed later in this statement.

OMB is required to submit an annual report to Congress on the performance of agencies in implementing FISMA. The report for fiscal year 2016 was released on March 10, 2017, and like previous reports, is available to the public on-line. Agencies are also required report to their appropriate committees on their FISMA performance, but those reports are not made publically available.

National Cybersecurity Protection Act

The National Cybersecurity Protection Act of 2014 (NCPA), statutorily authorized the National Cybersecurity and Communications Integration Center (NCCIC) within DHS.[2] Enacted during the 113th Congress, this law established the NCCIC as the interface between the civilian Federal Government and non-Federal entities for information sharing, risk analysis, and mitigation strategies related to cybersecurity. The law also permits DHS to provide technical assistance to both Federal and non-Federal entities to support risk management and incident response, conditional upon the request of that entity.

Cyber Security Act of 2015

The Consolidated Appropriations Act of 2015 was the vehicle for the Cybersecurity Act of 2015. Enacted by the 114th Congress, this law contains four separate titles, the first of which is the Cybersecurity Information Sharing Act (or CISA).[3]

CISA authorized an information-sharing program whereby cybersecurity threat information can be quickly, readily, and voluntarily shared among the private sector, between the private sector and the Federal Government, and among Federal Government agencies. CISA included provisions for the minimization of personally identifiable information, prohibitions on the Government use of that data, protections for the private sector from anti-trust concerns, and liability protections for sharing information. The law also authorized the application of defensive measures to mitigate known threats or security vulnerabilities on any network for which they own or have consent to take those measures from the network owner.

The second title is on National Cybersecurity Advancement. This part of the law provided authority for the NCCIC to manage the information-sharing program authorized by Title I. Title II also provided authority to DHS to provide, with or without reimbursement, the ability to detect and block threats coming from the public internet to agency networks. This capability is known in the cybersecurity community as intrusion detection systems and intrusion prevention systems, and as the National Cybersecurity Protection System (NCPS) or EINSTEIN (the name of the program DHS runs to deliver this capability). Title II also authorized DHS to develop and deploy tools to agencies which would continuously monitor the network activity of agencies' internal networks in order to detect risks and recommend mitigation activities. This is known as the Continuous Diagnostics and Mitigation program at DHS.

Title III, or the Federal Cybersecurity Workforce Assessment Act of 2015, requires Federal agencies to identify the cybersecurity workforce roles of greatest need to the Department and report to Congress on the progress of implementation.

Title IV contains miscellaneous cybersecurity requirements, including a study from DHS on the risks facing first responder networks.

ROLES AND RESPONSIBILITIES

To take an organizational view, these laws established certain roles and responsibilities among Federal entities for the security of the .gov domain. It may be helpful to think of OMB as the "strategic," DHS as the "operational," and individual agencies as the "tactical," with roles for NIST and agency Inspectors General, as well.

OMB, exercising its oversight of agency budgets, is responsible for overseeing agency adoption of cybersecurity practices and guiding agencies have a cybersecurity

[1] Pub. L. 113–283.
[2] Pub. L. 113–282.
[3] Pub. L. 114–113.

posture commensurate to their risk. Through their budgetary authority, OMB enforces the adoption of cybersecurity practices by directing the expenditure of funds for this purpose. OMB may also install new senior officials to oversee mismanaged cybersecurity programs, but CRS was unable to find an instance of OMB exercising that authority.[4]

DHS oversees agency adoption of cybersecurity programs, provides tools to protect agency networks, and coordinates Government-wide efforts on Federal cybersecurity.

Ultimately, however, agency heads are responsible for ensuring that risks are effectively managed in their own agencies, with cybersecurity being one such risk (financial and operational risk are among the others). In accordance with FISMA (Pub. L. 113–283) agency heads shall ensure the responsibility for cybersecurity is delegated to senior official, frequently a chief information security officer.[5]

NIST develops standards (i.e., the Federal Information Processing Standards) and guidance (i.e., Special Publications) to inform agencies of security practices to adopt.[6]

Inspectors General annually evaluate their agency's cybersecurity programs and provide recommendations on improving their agency's cybersecurity posture.

POLICY OUTCOMES

Prior to the 113th Congress, cybersecurity risks were one of many risks that an agency head was responsible for managing, along with fiscal risk and operational risk. In managing cybersecurity risk, agencies had a responsibility to manage risk effectively, and through their collective risk management the security of the .gov domain was obtained. DHS, OMB, and NIST provided programs, information, tools, and guidance to assist agencies in managing that risk, to include EINSTEIN and FISMA guidance.[7] However, it was incumbent upon the agency to accept those tools and implement that guidance.

With the passage of the aforementioned laws enacted in the 113th and 114th Congress, including the Cybersecurity Act of 2014, Congress updated law to reflect that risk exists not just at the agency level, but across the entire Federal Government. Federal agencies face cybersecurity risks not just for the information that individual agencies possess. Agencies also face inherent cybersecurity risks because they exist as part of the Federal Government, regardless of the work of that particular agency.

The Congress statutorily affirmed the role of DHS in mitigating risk to all Federal civilian agencies, reflecting the interdependent and inherent shared cyber risks agencies face. Rather than distribute risk mitigation across agency heads as their responsibility, DHS was granted authority to monitor cybersecurity risk for the .gov domain, provide tools to mitigate that risk, and assist agencies in doing so. With these authorities, DHS provides defense of agency networks at the transition point from the public internet to the agency's networks with EINSTEIN, which improves network security.[8] DHS also provides advanced vulnerability management with CDM.[9] These tools are designed not only to strengthen security of agencies where they are deployed, but also to the Federal enterprise by allowing DHS visibility to network activity across all Federal agencies. This is intended to allow DHS to notice malicious activity at one agency and the opportunity to mitigate that activity at another agency before it becomes disruptive, a form of herd protection for civilian agencies. Additionally, by consolidating these responsibilities at DHS, DHS is arguably able to monitor risk to the .gov domain and take action to mitigate that risk, freeing up agency resources to focus their risk at the agency level (i.e., the agency network, agency computers, and data).

The distinction between the Federal enterprise and the agency's enterprise appears to be continuing under the new administration. The President's "Budget in Brief" requests $1.5 billion for DHS cybersecurity mission (to be split between their .gov and private sector security operations, but explicitly support a "more assertive

---

[4] 40 U.S.C. § 11303.

[5] 44 U.S.C. § 3554(a)(3)(A).

[6] NIST, "FIPS Publications," website, October 16, 2015, at *http://csrc.nist.gov/publications/PubsFIPS.html*. And NIST, "Special Publications," website, April 8, 2016, at *http://csrc.nist.gov/publications/PubsSPs.html*.

[7] The e-Government Act of 2002 (Pub. L. 107–347) requires OMB to develop and issue guidance on implementing information technology security, and the Comprehensive National Cybersecurity Initiative (*https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative*) directed DHS to develop and deploy EINSTEIN to agencies.

[8] *https://www.dhs.gov/einstein*.

[9] *https://www.dhs.gov/cdm*.

defense of Government networks.").[10] Early indications from the administration officials signal that the position of the administration is to manage risks to the Federal enterprise as a single entity.[11] Through this strategy, the administration seeks to alleviate agency heads from having to further divide limited agency resources between mission operations and mission support, with the potential detriment to spending on the agency's cybersecurity. By shifting some additional cybersecurity actions from individual agencies to a single entity responsible for the security of all agencies the intent is to allow agencies to focus their resources on executing against the agency's mission.

Binding operational directives (BODs) are an example of the policy shift enacted with this group of legislation. These directives are compulsory direction to an agency from DHS to take specific action in order to protect the agency's information technology.[12] This is a unique relationship wherein one cabinet agency can direct another to take action—in this case, expend that agency's resources—for the purposes of managing risk to that agency, not risk to DHS. DHS is under no obligation to notify the public or Congress on the issuance of a BOD or its contents.

Mr. RATCLIFFE. Thank you, Mr. Jaikaran.

I now recognize myself for 5 minutes for questions.

Ms. Manfra, I want to start with you. As we have heard today, there have been a number of critiques of DHS's NCPS, or its principal component, EINSTEIN and CDM and their capabilities over the last few years. So some of those critiques relate to the holistic effectiveness of the capabilities, with respect to a cyber defense system and the lack of integration.

We have heard some concerns about the programs' limited ability to rapidly detect and disrupt breaches and specifically EINSTEIN 3A, signatures being limited and not being able to prevent some of the most advanced persistent threats.

So what is your response to that? How do you address that? What is DHS's mitigation, to the extent you think those are valid? I will give Mr. Wilshusen and Mr. Jaikaran a chance to weigh in, depending on your response.

Ms. MANFRA. Thank you for your question, sir. If I may just separate the two programs because I think the critiques are somewhat different.

For the National Cybersecurity and Protection System, which Mr. Wilshusen summarized in the GAO report, we did concur with the recommendations from the GAO report. We have also done some independent studies as well within the Department, leveraging MIT and Lincoln Labs to look at the system as well.

For National Cyber Protection System, if I may briefly review, it is made up of five capabilities. The first is intrusion detection, which is EINSTEIN 1 and 2. Those have been in place for quite a while.

Those are Unclassified capabilities that look at network flow and detecting known threats from traffic that is exiting and incoming to the network.

EINSTEIN 3A, as we refer to it, takes Classified information and uses it to protect Unclassified data that is traversing in and out of the agency's network by partnering with the internet service providers that service those agencies.

---

[10] OMB, "America First: A Budget Blueprint to Make America Great Again," budget report, 2017, at *https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/2018_blueprint.pdf*.

[1] Tom Bossert, "Cyber Disrupt 2017," remarks via video, March 15, 2017, at *https://www.csis.org/events/cyber-disrupt-2017*.

[12] 44 U.S.C. §3553.

The other two capabilities is the core infrastructure that supports everything that we do at, within the National Protection and Program Directorate and as well as our information sharing.

So the criticism is largely focused on EINSTEIN 3 Accelerated, which is the focus on being able to deploy quickly which we believe that was a valid criticism.

We were able to accelerate that deployment, and in cooperation with yourselves in the passage of the Cybersecurity Act that required agencies to deploy that. As I noted, we are now at 93 percent. So we believe that we are improving on the coverage aspect.

We are still working to ensure that the Classified indicators are as valuable as possible. We continue to work with our partners in the intelligence community and with network owners and operators to ensure that not only are the indicators valuable but, as Mr. Wilshusen noted, that we and our analysts are providing appropriate context for agencies to understand what should they do once they do receive an alert. So we are continuing to refine our processes there.

On the lack of integration between CDM and EINSTEIN, we also recognize that as a valid criticism. We integrated the two programs so that they are now managed under one program director. We believe that, from a programmatic perspective, that has resolved a lot of the challenges.

Then, technologically, what we hope to achieve is as CDM is deployed and we gather insight on what is going on inside of the networks, that we then correlate that with the threat information and the data that we are receiving on what is going on that is going in and out of the agency networks on the network traffic, and that we will then be able to provide our intake and analysts with a holistic risk picture on both the vulnerabilities and the threat that our two major programs are seeing.

But we also look to understand all of the available datasets for us and ensure that our analysts are taking advantage of those when they are providing that context.

Mr. RATCLIFFE. Thank you, Ms. Manfra.

So Mr. Wilshusen and Mr. Jaikaran, you heard Ms. Manfra essentially confirm some of the critiques. Very quickly, the mitigation path that she outlined, do you think that is reasonable?

Mr. WILSHUSEN. Yes, I do. It is something that we have been working with DHS since we issued our report back in January 2016. It has been over a year. We have been working with DHS and following their actions to implement our recommendations, and we will continue to do so until they are fully implemented.

Mr. JAIKARAN. So Ms. Manfra—sorry. Ms. Manfra highlighted one of the challenges with the sharing information. Once that information is shared it is reliant on the recipient of that information to take some action. That is the next step that the work that the analysts will perform to help agencies take the action to remedy the cybersecurity threats.

Mr. RATCLIFFE. My time has expired. I may have some additional questions in a follow-up round if we get the chance.

But at this time, the Chair now recognizes the Ranking Minority Member of our subcommittee, Mr. Richmond, for 5 minutes.

Mr. RICHMOND. Thank you, Mr. Chairman.

This is to Ms. Manfra and Mr. Wilshusen. In past reports, GAO has underscored the need for a more strategic approach to cybersecurity within the Department of Homeland Security. I authored a law last year that required DHS to create such a strategy and submit it to Congress.

Ms. Manfra, the statutory deadline for this strategy was March 23. What is the status of this strategy and when should we expect to see it?

Mr. Wilshusen, are there areas where a DHS-wide cyber-strategy, in your experience, will be beneficial to the Department as it carries out its diverse cybersecurity mission?

Ms. MANFRA. Thank you for your question, sir. We are working on the cybersecurity strategy as required under the National Defense and Authorization Act, recognizing that it was due last week.

However, we do need time to ensure that the new administration has an opportunity to review and provide guidance on what that strategy should look like. So we do anticipate that that will be over to you all soon. We look forward to working with you on implementing that strategy.

Mr. WILSHUSEN. Yes, I think the strategy should address several issues, including, of course, DHS's statutory responsibilities that it has with improving the security over the Federal Government. As part of that it should also identify the resources, the staffing that will be needed to implement that strategy and perform the functions that have been laid out to it under law.

So certainly clearly identifying its roles and responsibilities and the resources necessary to perform those activities, such as CDM and EINSTEIN, and the red and blue teaming exercises that it does, as well as the threat integration and information-sharing activities should all be addressed in that strategy.

Mr. RICHMOND. Ms. Manfra, do you have an estimate of how soon we would get it, a month, weeks?

Ms. MANFRA. Our goal is to get it within the next couple months, sir. But we do need to ensure that our leadership and the new administration has a chance to review it and provide the guidance. But sir, we are working very hard on it. This is something that we recognize as critical to our success in the next evolution for DHS cybersecurity.

Mr. RICHMOND. Thank you.

Then this is to the full panel. You can answer in whatever order you want. One of the obstacles DHS encountered during the Obama administration was convincing other Federal agencies to take advantage of DHS tools, like EINSTEIN and CDM.

Mr. Jaikaran, please explain how laws like the Cybersecurity Act of 2015 and FISMA have clarified agency responsibilities?

Mr. JAIKARAN. Thank you for the question, sir. Following the spat of legislation that was passed during 113th and 114th Congresses, there was that change whereas agencies were offered the tools by the Department of Homeland Security. However, it was incumbent upon that agency had to accept that tool and deploy it upon their networks.

After the change during the 113th and 114th Congresses, the acceptance of those tools, particularly the National Cybersecurity

Protection System or EINSTEIN, as the tools are known, was required.

You saw the change between the 30-some-odd percent to the 90 percent adoption from agencies when Congress statutorily required agencies to deploy that technology.

Mr. WILSHUSEN. I would agree. It had a very positive effect in compelling agencies to implement those programs.

Ms. MANFRA. Sir, I concur with the other two, and I would also note that it was able to remove a lot of the barriers that we had previous legal misperceptions that we had with agencies so that further facilitated the adoption.

Mr. RICHMOND. In a follow-up to that, from your perspective, how helpful have these laws been at raising the level of cybersecurity awareness across the Federal Government? What are some of the most pressing challenges that still remain?

Ms. MANFRA. Sir, I think the laws have been effective in raising awareness amongst the Federal leadership and the broader community that supports the Federal Government in securing our systems whether they are commercial or inside the Federal Government.

I think some of the major challenges continue to be how the Federal Government is able to modernize our IT systems and being able to protect legacy IT systems.

It is a continuing challenge, and it is resource-intensive which leads to the second challenge, which is resources. Being able to allocate sufficient resources to protecting that data in those systems that support that data continues to be a challenge.

Mr. RICHMOND. If you can answer this in, like, 2 seconds, just because you raised it, where are you all in the proposed budget? Are you all left alone, increased, or cut?

With this, Chairman, I——

Ms. MANFRA. Sir, you are referring to the fiscal year 2018?

Mr. RICHMOND. Yes.

Ms. MANFRA. The proposed budget blueprint does give us an increase at DHS.

Mr. RATCLIFFE. The Chair now recognizes the gentleman from New York, Mr. Donovan, for 5 minutes.

Mr. DONOVAN. Thank you, Mr. Chairman.

To follow up with my friend from Louisiana's questioning, you all spoke about the successes of the Cybersecurity Act of 2015 and the prior two pieces of legislation that came out of this committee and then eventually passed the House and the Senate and was signed into law. What else do you need?

What would you like to see us do going forward now in helping you protect our data, our network infrastructure? What is it that you would like to see us do, this committee, our whole Committee at Homeland Security and all of Congress to do to help you do your job better?

Mr. WILSHUSEN. Well, one thing I would say is to continue to shine a bright light on this issue. Hold hearings and have agency personnel come up here and testify on how they are implementing the requirements under these laws and how effectively they are doing that.

I think shining the light on that really raises the attention levels at the top levels of agencies and that helps to get actions completed at those agencies. So that would be one of the areas to do.

I will also point out that in another area where the laws have been beneficial is with the cybersecurity work force assessment initiatives that have been specified in a couple laws for DHS specifically and across the Federal Government where agencies are supposed to identify their critical cybersecurity talent gaps and take steps to fill them.

So those are a couple areas where I think you have done a job to help improve security.

Ms. MANFRA. Echoing Mr. Wilshusen's comments, I would agree with those. In addition, I think work on acquisition reform is important. A lot of the challenges that we face in deploying and procuring best-in-class technologies is not just for DHS but for the entire government, is very important in continuing to focus on building not just a Federal work force for cybersecurity but a National work force for cybersecurity that the Federal Government can benefit from.

Mr. JAIKARAN. Sir, my fellow panelists have highlighted a range of policy options that are available for the Congress. I think that is one of the unique areas of this space, cybersecurity, that issues of work force, issues of IT acquisitions and modernization, issues of oversight all play into this issue of cybersecurity and our options for the Congress to consider moving forward.

Mr. DONOVAN. Can you explain to me what the acquisition problems are that maybe we can address?

Ms. MANFRA. I think for us, a lot of what we are looking at is, one, ensuring that we are leveraging the authorities that we currently have and improving our processes to ensure that those are as innovative and rapid as possible. So we are making and we are doing that work inside the Department and encouraging other agencies to do the same.

But I do believe that looking at processes that would enable faster tech refresh of our capabilities within the Government and identifying opportunities to work with non-traditional Government contractors.

There are still some barriers in the way that the acquisition is currently written and done that doesn't allow us as easily and as rapidly to engage with those entities.

Mr. WILSHUSEN. I think I would just add to it is kind of following the example what we are doing under CDM program, and that is leveraging Government-wide demand for products to buy in volume and so we are able to achieve cost efficiencies through volume discounts.

So for many different types of information security-related tools and capabilities, to the extent they can be acquired across the entire Government and all agencies can share will be a very positive step, not only from a cost-effectiveness purview, but also from a standardization view, too. That could also help allow for greater integration of the computing environments across the Federal agencies.

Mr. JAIKARAN. I have nothing to add to the comments of my fellow panelists.

Mr. DONOVAN. I have 30 seconds left, and I want you to understand you are speaking to a guy whose VCR still flashes 12. So in layman's terms, is there any laws that we can create for you that protects our data, protects our networks better?

You seem very satisfied with what this committee, what this whole committee with Congress, has done so far in the area of cyber. Is there something that you would love to see us do?

Ms. MANFRA. From our perspective, sir, ensuring that DHS is organized to achieve our cybersecurity mission. Renaming our organization so people understand what the National Protection and Program Directorate is really very important for us. We look forward to working with the subcommittee and the committee on that.

Mr. DONOVAN. Thank you. My time has expired.

Mr. Chairman, thank you.

Mr. RATCLIFFE. The Chair now recognizes the gentleman from Louisiana, the Ranking Minority Member of the committee, Mr. Thompson—or Mississippi.

Mr. THOMPSON. Well, I will take Louisiana, but I am from Mississippi.

Mr. RATCLIFFE. Is there a difference?

Mr. THOMPSON. Not really. Thank you, Mr. Chairman.

All of you talked about the capacity of having cyber experts within Government. One of the criticisms we hear quite often is we don't have enough, or as soon as we get them, the private sector acquires them. I could use another term, but——

So Ms. Manfra, what do you think we need to do, that we are not doing, to recruit and keep cyber professionals within the Federal Government system?

Ms. MANFRA. Thank you, sir, for your question. This is something that is not only critical for us but something that I personally care a great deal about. As a part of the broader initiatives to improve STEM education in the United States, I believe cybersecurity is an important component of that.

We at the Department have done a lot of work to encourage universities and working with NSA and the NSF to have a common curriculum that universities will adopt and developed a program with the Office of Personnel Management called the CyberCorps Scholarship for Service that allows graduates of that program to benefit from a scholarship and then come and work for either Federal, State, and local government.

That is one area that we have seen tremendous benefit from. While they may leave the Government after their time is up, we appreciate the time that they did spend with us.

We also are looking in terms of the authorities that this Congress gave us to create an accepted service for cybersecurity. We are moving forward in developing the components of that so that we can begin transitioning to that excepted service, which will allow us to drastically change how we can keep up with the marketplace on cybersercurity personnel.

But while we are working to implement that, we have worked to, within our current authorities, use what we can to retain the best and the brightest that we have right now, by ensuring that with the tools that we have at the moment to retain them and provide them with a better, a market-based approach to their salary.

There is more work to be done, but this is something that we have done a lot, and we look forward to——

Mr. THOMPSON. Well, you have given me a broad, broad response to my question. Let me tell you what I hear from a lot of Government employees. They will say because there is a private contractor with an employee sitting next to me, and as we talk I find out that we are doing the same work.

But that private contractor is probably making one-and-a-half times, if not more, than my salary as a Government employee. So that impacts morale and a lot of other things. So do you hear that, too?

Ms. MANFRA. Absolutely, sir, and the retention incentive program that we have put in place for now, while we work to implement the full excepted service, has actually had a drastic effect in reducing our attrition rate so that we were at about a 13 percent attrition rate. We are now down to a 9.

We think that that is commensurate with industry. We did absolutely hear that quite a bit and we recognize that, and we are using our tools to——

Mr. THOMPSON. You know, we even said go out and hire 1,000 people if you can find them and plus-up the Department because you are short. I don't think we quite accomplished our goal. Maybe you can help me?

Ms. MANFRA. Yes, sir. Recruiting is still a challenge. We believe we have made progress on retention. We are also looking at innovative ways to recruit, and we do have some direct hire authority that we don't believe that we were fully leveraging.

So we have worked with industry to look at how they recruit talent to the technology companies there. We are looking at adopting a lot of those practices in our human capital process.

Mr. THOMPSON. Well, I look forward to the next conversation and you tell me how good we are moving in that direction.

Ms. MANFRA. Absolutely, sir.

Mr. THOMPSON. OK. Thank you.

Mr. Wilshusen testified that the EINSTEIN program is good if we know the militia's signatures. I guess the question is what do we have as the alternative when we don't know what the signatures are? Maybe you can tell me, and then I will go to Mr. Wilshusen?

Ms. MANFRA. Absolutely, sir. We think that, as I noted briefly, that there are three areas that we want to focus on. One is ensuring that we have better signatures. Signatures are still a useful capability to deploy.

So we want to ensure that we have the best signatures that are available and that we are using our private-sector partnerships to both increase the quantity and the quality of those.

We also want to ensure that the agencies understand how, whether, it is not just a black or a white. This is either bad or this is good.

But we want to look at those signatures and give them information about how likely the severity of the threat is, which we refer to as reputation scoring. This is something that industry also uses.

The third one is what we refer to as anomaly-based detection. That is more challenging. The technology does exist in the industry and we are piloting it. But it is a challenging capability.

We have seen success with some of our early pilots and we look forward to understanding from those successes and learning from where the challenges were to fully deploy that capability.

Mr. THOMPSON. So is that the pilot that we should have concluded last July?

Ms. MANFRA. The pilot was begun in early last year. We are still in the pilot phase.

Mr. THOMPSON. So it appears——

Ms. MANFRA. We brought it. We brought in the pilot, sir. One of the things that we need to continually be mindful of is our ability to scale technological deployments.

So just because something might work at one agency we need to ensure that it can scale for the entire civilian government. So we expanded the pilot from that first agency to include others.

Mr. THOMPSON. All right. Thank you.

Thank you, Mr. Chair.

Mr. RATCLIFFE. The gentleman from Mississippi yields back.

The Chair recognizes the gentleman from Pennsylvania, Mr. Fitzpatrick.

Mr. FITZPATRICK. Thank you, Mr. Chairman. Thank you to the panel for being here.

I will start with Ms. Manfra and then second to the entire panel. The relationship with the FBI, would you describe it as one of cooperation, one of competition or both, knowing that there are multiple agencies in the same space? Sometimes that can help and hurt.

Second for the panel, we repeatedly hear the same four nations mentioned through testimony here, Russia, China, North Korea, and Iran. How would you describe to this committee the uniqueness of each of those cybersecurity threats that each of those nations pose? How would you rank them?

Ms. MANFRA. The question of the FBI cooperation, I am very proud that I consider this an area of cooperation. Now, that doesn't mean to suggest that there aren't areas where we have different equities. But that is appropriate.

We believe that we have built the capabilities to work through those processes so that we ensure that they are able to pursue their investigative equities and we are able to pursue our network defense.

We have FBI sitting on the NCCIC floor 24/7, and we routinely work with them to ensure that we are both aware of the same reporting streams, whether it is through their sources or through our partnerships, and that we are continuing to cooperate on mitigating and preventing potential incidents and working together to reduce the consequences should an incident occur.

PPD–41, which was a policy that was delivered at the end of the last administration, laid out the doctrine that is still valid and that we still work under where the FBI leads what we refer to as the threat response. That is containing the threat.

Where we lead what we refer to as asset response, which is working with the victims and understanding the broader risk and how we mitigate that. We believe that works very well.

Mr. WILSHUSEN. With respect to the four nations, I would say that Russia is very skilled, capable, and is probably more surgical in its intrusion capabilities and intense.

China also has a lot of skills but and is probably takes a broader base view in trying to get into more different activities across the Government and the economy.

I would just say probably Korea and Iran are more likely to be involved in more destructive activities, that they have that capability.

Mr. JAIKARAN. Sir, unfortunately my work at CRS has not provided me insight into the capabilities of each of the countries. However, I do have colleagues who do study threat actors specifically, and I would be happy to get them in contact with you after this hearing.

Mr. FITZPATRICK. Thank you.

I yield back.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for your testimony today and most especially what you are doing to secure our networks against those who have bad intentions.

So Ms. Manfra, if I could start with you? So DHS was authorized by FISMA 2014 to use binding operational directives to issue mandatory instructions to agencies regarding cybersecurity policies, measures, standards, and guidelines.

So far how many of those binding operations directives have been issued? Can you also characterize the response of the Federal agencies to these directives and also identify where their enforcement can be improved?

Ms. MANFRA. Thank you, sir. We have issued four binding operational directives to date. We believe that they have been very effective. They were all delivered by former Secretary Johnson to his peers, which we do believe is part of the success of these directives.

We made very deliberate decisions to do our best to issue binding operational directives that would enable us to measure their success in implementing those directives.

The first directive on reducing critical vulnerabilities and the one on high-value asset and participating in the high-value asset assessments, as well as closing some vulnerabilities related to later revelations of activity with some criminal tools that were being used, have all been very effective.

The critical vulnerability we have excellent data that shows that not only are they closing those critical vulnerabilities, but they are reducing the time to close those vulnerabilities. We gave them 30 days to close those critical vulnerabilities. Many of those vulnerabilities had been open for oftentimes more than a year.

We are now seeing a dramatic reduction in the amount of time that it is taking them to reduce those critical vulnerabilities, which

we think is a demonstrable change in behavior and recognizing the value of those binding operational directives.

Mr. LANGEVIN. So in all four cases the binding operational directive was satisfied and the agencies closed the vulnerabilities, addressed the problem?

Ms. MANFRA. Yes, sir. We did not close the critical vulnerability or the high-value asset one because those were ones where we wanted to continue to be able to measure them.

So we work with them, their chief information officer and chief information security officer to continue to provide them reports on the status because we believe those are always valid directives for them to follow.

Mr. LANGEVIN. OK. Thank you.

Mr. Wilshusen, has GAO studied the impact of binding operational directives issued by the Department?

Mr. WILSHUSEN. We have not.

Mr. LANGEVIN. OK.

So Ms. Manfra, we recently, we heard recently before the committee that the threat indicators are shared by DHS, often lack context that make private-sector participants, that they would make them—may desire to make them actionable.

At the same time developing such context takes time and in the development of the Cybersecurity Act of 2015 we heard that rapid sharing was essential. So how does the Department balance the competing needs of sharing actionable information with appropriate context against the desire to share quickly?

Ms. MANFRA. Thank you, sir, for that question. We believe that all of those are valid requrements. However, not all of our stakeholders require all of those various different capabilities.

Our automated indicator-sharing program is to get as much threat information out as quickly as possible in an automated way so that people can ingest those indicators and protect themselves.

We believe that that has been a successful program. We are about a year into it, and we have nearly 200 participants that are receiving indicators from us.

Now, there is always feedback and we appreciate the feedback in the working to improve that program. We also have other programs to include providing private sector with clearances so that we can work with our intelligence community partners to provide Classified briefings should the threat require it.

We also work with our cyber information-sharing and collaboration program where we can do technical exchanges with analysts at industry organizations that have significant capabilities of their own where we can exchange broader information on context and refine what it is we are doing. That is how we think of focusing our efforts.

Mr. LANGEVIN. So the people that we have been talking to, just so you have some feedback, didn't think that the information sharing has been all that effective. So we need to work harder in that area.

I would ask you now if you have a secondary process? I mean, sharing quickly the indicators is important and getting that out is important. But what about a follow-up and helping to share context in a second round?

Ms. MANFRA. Absolutely, sir. Similar to what we are doing with the Federal agencies is to help score some of these indicators working with the private sector to ensure that we are providing both the quality quickly and understanding that we may need to follow up either broadly with an entire sector or on specific entities that are being targeted to provide them with additional context so that they can make threat decisions.

But we have heard similar feedback. We understand from our partners that we are improving, but that we do need to continue to improve on this capability.

Mr. LANGEVIN. Thank you.

I know my time has expired, but just in closing, Mr. Wilshusen, I hope that GAO would look at these binding operational directives issued by the Department, especially since there are only four, and give us an assessment.

It would certainly help the committee to decide whether the binding operational directive is meaningful or not. We appreciate the testimony of Ms. Manfra, but I would be——

Mr. WILSHUSEN. I will be happy to work with your staff to look at that.

Mr. LANGEVIN. Thank you.

Thank you, Mr. Chairman, I yield back.

Mr. RATCLIFFE. We have a number of Members that have competing hearings this morning and haven't been able to make it back. So I know that they are going to have questions for all of you that will be submitted in writing.

So with that, however, I will thank the witnesses for your testimony today. I want to thank the Members for all their questions. As I said, Members of the committee will have some additional questions, and we will ask you to respond to those questions in writing respectively.

Pursuant to committee rule VII(D), the hearing record will be held open for 10 days. Without objection, the subcommittee now stands adjourned.

[Whereupon, at 11:16 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR JEANETTE MANFRA

Question 1a. Do the objectives for CDM still align with reality of the evolving cyber risks faced by the Federal Government?

On March 22, the committee held a hearing where Members heard about the rapidly-evolving nature of cyber threats. Based on this changing threat landscape how is DHS ensuring CDM tools and capabilities are keeping up with the evolving threat landscape?

Question 1b. How is DHS ensuring that CDM tools and capabilities are addressing the devices and end-points that pose the most risk to Federal agencies going forward?

Answer. The Continuous Diagnostics and Mitigation (CDM) program objectives directly align with the reality of evolving cyber risks, and the program is committed to continuing to assess its effectiveness at addressing such risks. In the context of ever-evolving cyber threats, there are basic fundamental steps to strengthening cybersecurity. For instance, knowing the information technology (IT) assets connected to and interfacing with agency networks, and therefore, must be managed is a crucial basic fundamental step related to cybersecurity. In the first phase of CDM, the National Protection and Programs Directorate (NPPD) is helping Federal agencies better understand what is on their network and better manage the cybersecurity of those assets. CDM works to ensure that agencies know what IT assets they operate and how well those assets are configured and patched. IT assets, combined with their vulnerabilities and misconfigurations, represent a significant attack surface that our adversaries target. Through better patching and configuration, agencies are able to reduce the likelihood of successful compromise against the evolving threat. This is one of the key objectives of CDM.

Another fundamental principle of CDM is to understand who is on the network. By learning who has access to agency networks, including those individuals with privileged user access, agencies can begin to appropriately restrict network access and ensure the principle of least privilege is being followed. This second phase of CDM is a significant step forward in managing cyber risk.

NPPD's National Cybersecurity and Communications Integration Center (NCCIC) will soon operate a Federal dashboard as part of CDM. Integration of the Federal dashboard into the NCCIC's 24/7 operations will provide DHS's cybersecurity operators with around-the-clock situational awareness into the current security posture of Federal agencies. This will enable the NCCIC to help agencies prioritize their patching and configuration actions to address the most critical vulnerabilities based on current threat data. It also allows the NCCIC to alert agencies when new threats arise that exploit specific vulnerabilities. The NCCIC will be able to adjust the criticality information related to specific vulnerabilities in order to bring agency attention to the worst problems that should be addressed first.

In order to maintain product currency, ensure innovation, and keep up with an evolving threat, on at least a quarterly basis CDM allows integrators to submit for review the latest tools that meet the CDM technical requirements. Once the tools pass technical review conducted by the CDM program, they can be added to the approved product list on the blanket purchase agreements, making them available for purchase and use at Federal agencies.

In working with Federal agencies and CDM integrators, NPPD is helping to ensure that CDM capabilities protect Federal agency networks. By providing agencies with significantly more visibility into their end-points and users, CDM is helping agencies continuously monitor their IT environments and improve their overall cyber hygiene. Agencies are now installing the tools across their networks, which gives their leadership and network administrators' visibility into the current state of their networks to better identify and prioritize areas of cyber risk, particularly those areas that pose the most risk.

Question 2. Is the Department providing technical training to agency system administrators on the use of the CDM tools so they know how to effectively and optimally use the tools to diagnose and mitigate vulnerabilities?

Answer. The Continuous Diagnostics and Mitigation (CDM) program anticipated training requirements for operation and management of capabilities. Training requirements were included in the contract solicitation. All CDM integrators are required to provide sufficient training to enable agencies to transition the CDM tools to agency operation once the integrator contract is completed. When transition is complete, agencies will be able to understand what the CDM tools are telling them about agency vulnerabilities via the agency dashboard, and respond appropriately.

Funds available for training are limited, and experience is showing that agencies are requesting more detailed, sustained training options. DHS has reminded agencies of the need to fund training for tools and governance activities. For dashboard operations, CDM is developing on-line, hands-on workshops in fiscal year 2017 to assist agencies with understanding how to use the CDM agency dashboard.

Question 3. Are departments and agencies being provided with thorough estimates of what the cost of maintaining the CDM products will be?

How is DHS working with departments and agencies on the transition to maintaining CDM products?

Answer. Yes. Since December 2015, the Continuous Diagnostics and Mitigation (CDM) program worked with the Office of Management and Budget (OMB) to provide cost estimates to agencies on all CDM capabilities provided to date. This information was updated again in December 2016. In the third quarter of fiscal year 2017, the program met with the chief information officer and chief financial officer or their designees, of each Chief Financial Officer Act agency [as listed in U.S.C. § 901(b)] to provide even more detailed cost estimates for license maintenance in fiscal year 8. We are working closely with OMB and agencies to ensure that agency budgets are able to absorb the tool and labor costs after the Department of Homeland Security transitions the CDM solutions to agencies.

Question 4. What feedback mechanism does the Department have for soliciting and receiving comments from agencies on their experience with the CDM program?

What benefits and challenges have the agencies identified with the program?

Answer. During the summer of 2016, the Federal chief information officer (CIO) held a CyberStat on the Continuous Diagnostics and Mitigation (CDM) program. The CyberStat included program documentation review, interviews conducted by Office of Management and Budget (OMB) staff with several agencies, and meetings between the Federal CIO and the CIO or chief information security officer (CISO) of each agency. This CyberStat was a valuable source of feedback. The Federal CIO noted that "all participants expressed support for the security objectives of the program and emphasized their commitment to procuring CDM Phase 1 tools."

Other benefits included:

- Establishing a consistent approach toward information security continuous monitoring of networks across the Federal civilian agency enterprise. The Federal Information Security Modernization Act of 2014 requires agencies to provide security for the networks that support the operations and assets of their agency and codifies the Department of Homeland Security's (DHS) authority, in consultation with OMB, to administer the implementation of information security policies and practices for civilian agencies. Through CDM, agencies receive a significant investment by DHS to boost previous efforts and, in many instances, are able to achieve an internally consistent enterprise approach, allowing them to leverage similar product knowledge, subject-matter expertise, and technical support across the agency.
- Pioneering an innovative acquisition approach by combining agencies into groups for similar requirements and project efficiencies. By grouping agencies, CDM is achieving economies of scale and reducing pricing for labor and products. To date, CDM has achieved cost avoidance of $600 million on products over the Schedule 70 pricing.
- Leveraging a consistent system engineering life cycle, tailored from DHS.
- Establishing an approach toward supply chain risk management across the Federal civilian Government enterprise. To date, the program has applied secure delivery controls for well over 1 million products delivered to participating agencies.

Challenges identified by some agencies included issues such as: Asset and infrastructure gaps; agency governance and management challenges; integrator project management challenges; training and knowledge management; entrance on duty requirements; and selection of tools and requirements. With regard to the identified gaps, agencies noted that CDM revealed a significant number of new end-points than previously understood, and unplanned infrastructure upgrades and moderniza-

tion may be required to support new CDM tool deployments. While the ultimate goal of CDM phase 1 is to identify all end-points on the network, these activities resulted in budget implications for DHS and agencies. Further, since additional end-points were identified, future-year license maintenance costs will increase. Governance challenges include the need for CIO engagement and leadership with clear project management. Integrator project management challenges were identified as requiring proactive engagement and communications with the agencies, and well-documented plans, schedules, etc. The program worked closely with each integrator to ensure plans and schedules were clearly communicated on a timely basis. Agencies identified a need for training and better knowledge management, particularly concerning the tools. Entrance on duty requirements were identified as causing significant delays in on-boarding critical integrator personnel, resulting in schedule delays. With regard to tool selection, some agencies noted that support for the awarded solutions varied within agencies.

The CDM program office has worked with OMB on the next steps, which includes implementing improvements and addressing concerns, as appropriate. Moving forward, CDM has established a Customer Advisory Forum (CAF) comprised of CISOs, or designees, from each agency in order to receive feedback on topics of interest and concern. The CAF will continue to meet on a bi-monthly basis and will serve as the focal point for interagency collaboration related to CDM planning and implementation, including customer proposals and adoption, organizational and technical challenges, acquisition planning, and capability integration priorities.

Question 5a. A number of stakeholders have raised a concern that there is some confusion among agency officials about the technology tools and solutions CDM directs them to use. Can you provide greater clarity around this, particularly as it relates to tools and solutions that Federal agencies may already have in place?

For example, if an agency has already procured and deployed an IT asset inventory and management solution, can the agency continue to use that solution and be in compliance with CDM?

Or would they have to scrap this already paid-for and deployed solution, and buy something from a CDM approved vendor?

Question 5b. How does DHS help officials at agencies across the Government understand whether they are able to use solutions they have already procured, or whether they will need to deploy new solutions through CDM?

What steps does DHS take to provide this clarity to agencies so that there isn't unnecessary duplication of effort, or unnecessary procurement of technology?

Answer. The Continuous Diagnostics and Mitigation (CDM) program does not prescribe which tools should be deployed to which Federal agencies, but rather defines a cybersecurity requirement and allows industry to propose a set of tools that comprise a CDM solution. The solutions are evaluated on a technical and cost basis with participation from agencies, the Department of Homeland Security's (DHS) CDM program, and the General Services Administration (GSA) Federal System Integration and Management Center (FEDSIM).

Solutions are awarded when identified as the best value to the Government. Historically, there have been niche buys of technology tools and solutions by parts of an agency without consideration of efficiencies that could be gained through enterprise-wide standardization, resulting in higher cost of ownership when that technology needs to be integrated into a bigger solution. The general principle of CDM is to gap fill by extending the product bases within an agency or component versus wholesale replacement—applying the best value principle. The best value principle takes into account re-use of existing tools, efficiencies gained through increased volume discounts on products, leveraging of shared resources with solution-specific expertise, reduced number of architectural baselines, and consistency of data reporting to agency and Federal dashboards. Among the lessons learned within Federal agencies was that the niche technology approach provided little enterprise visibility of the agency network.

CDM seeks to find best value solutions in cooperation with Federal agencies. In instances where an integrator proposed a solution to meet a specific requirement that conflicted with an existing agency capability, the agency had a choice to accept the CDM-provided solution, along with installation and integration labor, or to retain its existing capability but assume the responsibility for integrating required data provided by existing agency tools into its agency dashboard to ensure achievement of CDM's goal of consistent data reporting between agency dashboards and the Federal dashboard across all agencies.

Prior to release of the request for proposals (RFP) during the solicitation phase of CDM, DHS has worked closely with agency officials to identify agency requirements, including, where appropriate and driven by the agency, considerations for agency-specific requirements. For the task orders on Phase 1 of CDM in 2014, DHS

helped agencies complete detailed technical spreadsheets that were provided to all bidders. The bidders were then able to consult agency-specific reading rooms where additional technical detail was provided. A similar mechanism was used in Phase 2 of CDM, where agencies were asked to list existing products on an attachment to the Phase 2 RFP to provide offerors a snapshot into the current agency landscape. As CDM moves into Phase 3, DHS is working with agencies to identify their priorities, which will help shape the capabilities DHS funds. DHS will continue to work with agencies through CDM's Customer Advisory Forum and other mechanisms to provide transparency and reduce duplication of effort.

CDM established a new vehicle, CDM DEFEND, to cover Phase 3 and beyond. This approach will continue to incorporate successful elements of the current CDM Blanket Purchase Agreement, such as reading rooms and Approved Product Lists, while moving away from a defined BPA to use of a Government-Wide Acquisition Contracts (GWAC), Alliant, managed by GSA. The GWAC approach will avoid the cost of establishing a new BPA, and provide greater flexibility for CDM to address evolving requirements as new needs are identified. This approach includes provisions for agencies to contract for agency-specific requirements directly if an agency has identified cybersecurity requirements that are not part of the CDM program.

Question 6. What is DHS planning to do to accelerate the adoption of new capabilities based on lessons learned to date?

If a deployed Phase 1 tool has embedded capabilities that have additional functionality, such as those in later phases, can an agency use that capability now?

Answer. As the Continuous Diagnostics and Mitigation (CDM) program works to replace the existing blanket purchase agreement task order, several factors will support accelerating the adoption of new capabilities. Shorter evaluation and award cycles for targeted capabilities beyond the base capabilities will allow an agency to tailor solutions and assess specific tools. Agencies' experience with targeted new capabilities will provide a better understanding of how broadly a specific tool can apply, potentially reducing the time to negotiate enterprise-wide solutions. Additionally, the process for adding new products to the approved portfolio is being significantly enhanced in order to reduce the time for availability from several months to potentially a couple of weeks.

The CDM integrator is implementing capabilities according to the phased CDM implementation schedule. If a tool deployed during Phase 1 has additional functions that are scheduled for later CDM phases, agencies are free to implement the additional functionality if they resource the work, fund the associated product and labor costs, and ensure tool configurations meet subsequent CDM requirements and compatibility with Federal dashboards.

Question 7. One common problem in information technology management generally is the issue of "shelfware"—that is, software that has been procured but never deployed. As we look across agencies and department, it is probably fair to say that many have acquired solutions that can achieve the requirements of CDM but they are sitting on a shelf somewhere and individuals at the agency are either unaware of these capabilities, or they have failed to deploy these capabilities. Is there a process that helps agencies better understand and utilize current assets that can meet CDM requirements?

If so, can you please describe how that process works?

Answer. Agencies can consult with the Department of Homeland Security regarding whether an existing tool, deployed or not, meets Continuous Diagnostics and Mitigation (CDM) program requirements. CDM publishes a product catalog through the General Services Administration (GSA), available on-line, that identifies CDM-approved tools. The CDM program has provided labor support to agencies who reported they already had existing products but did not have them deployed. Since these products were part of the CDM solution, it was deemed in the best interest of the Government to ensure they did not remain "shelfware." In future phases, CDM will continue to maintain approved product lists that crosswalk CDM-approved tools to CDM capabilities. Additionally, CDM will offer contract vehicles that agencies can use to fund installation, configuration, and integration activities associated with existing, legacy products. Although DHS provides cybersecurity tools and services, the responsibility of employing those tools and services for the practice of cybersecurity is ultimately the responsibility of each agency. It is incumbent on each agency to engage with CDM in order to fully utilize available resources.

Question 8. CDM seeks to provide threat protection at the network boundary. How is DHS ensuring this protection extends across all levels (or tiers) of agency infrastructure, especially when the intensity and scale of threats is increasing exponentially?

Answer. EINSTEIN, the Department of Homeland Security's (DHS) intrusion detection and prevention capability, provides perimeter defense for Federal civilian ex-

ecutive branch agencies. However, EINSTEIN will never be able to block all malicious cyber activity. EINSTEIN must be complemented with systems and tools inside agency networks, such as Continuous Diagnostics and Mitigation (CDM), and by proactive efforts from each Federal agency to implement cybersecurity best practices, such as multi-factor authentication and employee training. DHS deploys tools that provide visibility into all levels of the agency networks to provide broad protection CDM Phase 1 is focused on "what is on the network" and CDM Phase 2 is focused on "who is on the network." CDM Phase 3, will be focused on filling gaps at the network boundary and developing on-going assessment and authorization across the agency systems. The objective is to address the evolving threat by extending external visibility into internal agency structures, further reducing unauthorized access to networks, systems, and data.

Prior to the deployment of CDM Phase 1 tools to agencies, agencies underestimated the number of devices on their network. The lack of full awareness by various agencies regarding "what is on their network" played a significant role in some of the challenges with CDM Phase 1 deployment, particularly the need to increase contract ceilings and identify funds to cover devices and end-points not previously identified, and at the same time underscored the program's value. The CDM Phase 1 deployments are now providing agencies with significantly more visibility into their end-points, enabling them to effectively manage and configure those end-points on the network.

Question 9. How will DHS continue enhancing cybersecurity defenses despite the added complexity and risk from the proliferation of mobile devices in the Government IT enterprise?

Answer. The Department of Homeland Security is constantly evaluating emerging technologies and working with Federal agencies to identify the most appropriate cybersecurity solutions. The utilization of mobile devices is driving changes in our network security designs.

As threats and technology evolve, the Continuous Diagnostics and Mitigation (CDM) program is working to incorporate cybersecurity solutions for new computing paradigms, such as mobile computing. At the time CDM Phase 1 was awarded, there was insufficient Federal policy direction for mobile security. From its inception, it was an objective of CDM to eventually address mobile security. Since then, there has been significant progress in the formulation of reference security architectures for mobile, and the program is planning to include mobile computing in the next generation of task order work.

Question 10. Does DHS intend to serve as a Federal agency advisor for mobile device authentication to better secure sensitive Government networks and data that leverages work DHS is doing on innovative Government smartcard and credentialing applications?

Answer. The Department of Homeland Security administers the implementation of Federal agency information security policies and practices, and provides recommendations and technical assistance on cybersecurity and resilience measures. Mobile security is part of this effort.

Question 11a. The Government knows that it needs to implement cybersecurity at the data and document level because existing cyber protection strategies are fundamentally inadequate. Phase 4 of the CDM program acknowledges this issue. What is the time frame to roll out data-level security measures for the DHS CDM program?

Have DHS and GSA considered accelerating the roll-out of data protection capabilities included in its CDM Phase 4 strategy?

Question 11b. What CDM training is taking place to ensure Federal agencies are planning and budgeting to adopt such "data-level protection" capabilities?

Answer. The President's fiscal year 2017 budget request included funding for a newly-proposed Continuous Diagnostics and Mitigation (CDM) Phase 4 to expand the CDM program to include additional tools and services to protect sensitive and high-value asset data within agency networks. While not fully funding the requested level, the fiscal year 2017 Consolidated Appropriations Act provided funds to begin the planning activities necessary to define CDM Phase 4 in preparation for an acquisition review in late fiscal year 2018. However, we are continually working to identify opportunities to accelerate and innovate within CDM and other cybersecurity-related programs at DHS and hope that we will be able to accelerate as appropriate.

There are fundamental technical steps that have to be in place prior to focusing on the data, such as identifying the assurance level on the user's identity and the degree of hardening and protections within the infrastructure that holds the data. This is done through the implementation of key parts of Phases 1, 2, and 3. Given

Phase 4 requirements have not yet been fully developed detailed planning to include training requirements have yet to be defined.

Question 12. The Trusted Internet Connection (TIC) was designed to provide an additional layer of perimeter security to Federal Government systems by consolidating internet points of presence and enabling network monitoring of traditional on-premises systems. Advancements in cybersecurity technology, specifically through cloud computing, have changed the security models that guided the original TIC design. Some have suggested that the TIC in its current form creates too many latency, scalability, and architectural issues that hinder the migration of workloads to the cloud and other emerging technologies. Does DHS plan to update TIC policy to allow these technologies to provide functional operational visibility?

Answer. The Office of Management and Budget (OMB) issues Trusted Internet Connection (TIC) policy. The Department of Homeland Security (DHS) is collaborating with OMB, Federal agencies, and industry to identify potentially effective and innovative means to both meet Federal security requirements and to ensure a level of resilience that aligns with agencies' risk decisions.

Question 13. Given the pressing cybersecurity mission DHS provides, what is the time line for resolving the DOMino procurement issue?

How does DHS plan to minimize DOMino transition risk, staffing, and impact to providing the Federal Government environment with critical cyber defense capabilities in light of recent events?

Answer. On June 9, 2017, the Department of Homeland Security (DHS) awarded the DOMino contract and the task order for Operations and Maintenance. The Design and Analytics Task Orders will be issued in the near future. DHS has put in place bridge contracts to support the transition from incumbent contractors to the DOMino vendor.

Question 14. Given the rapid rise in the threat landscape and the increasing attack surface for the U.S. Government, has the CDM initiative kept pace and is it capable of introducing solutions expeditiously to combat and protect?

Given the fact that the Federal workforce has become more dependent on "cloud" and "mobility," is CDM still the correct solution to address threats posed in the cloud and mobile spaces?

Answer. In order to maintain product currency, ensure innovation, and keep up with an evolving threat, on at least a quarterly basis, the Continuous Diagnostics and Mitigation (CDM) program allows integrators to submit for review the latest tools that meet the CDM technical requirements. Once the tools pass technical review conducted by the CDM program, they can be added to the approved product list on the blanket purchase agreements, making them available for purchase and use at Federal agencies.

As threats and technology evolve, CDM is working to incorporate cybersecurity solutions for new computing paradigms, such as cloud and mobile computing. At the time CDM Phase 1 was awarded, there was insufficient Federal policy direction for cloud and mobile security. From its inception, it was an objective of CDM to eventually address cloud and mobile security. Since then, there has been significant progress in the formulation of reference security architectures for both, and the program is planning to include both cloud and mobile computing in the next generation of task order work.

Additionally, CDM is assessing the movement to different detection methods and countermeasures to threats that are not pre-defined, or are behavior versus signature-based.

QUESTIONS FROM RANKING MEMBER CEDRIC L. RICHMOND FOR JEANETTE MANFRA

Question 1a. The Federal Information Security Modernization Act, Pub. L. 113–283, grants the Secretary of Homeland Security authority to issue "binding operational directives" to direct other agency heads to take specific actions to protect their networks.

What factors go into the decision to issue a directive? If you have a formal criteria, please provide a copy.

Question 1b. How has DHS used this authority thus far, and how do you assess how effective each directive has been?

Question 1c. In the view of the Department, would it be an appropriate exercise of this authority for DHS to direct specific action to encourage better cyber hygiene going forward, rather than address specific known risks?

Answer. The Secretary of the Department of Homeland Security (DHS), in consultation with the Director of the Office of Management and Budget (OMB), has the authority under 44 U.S.C. § 3553(b)(2) to develop and oversee the implementation of binding operational directives (BODs). The Federal Information Security Mod-

ernization Act (FISMA) statute includes specific topics for BODs, including requirements for reporting security incidents to DHS's National Cybersecurity and Communications Integration Center (NCCIC), requirements for the contents of the annual FISMA reports, requirements for the mitigation of exigent risks to information systems, and other operational requirements as OMB, or DHS in consultation with OMB, may determine are necessary.

DHS, acting through the National Protection and Programs Directorate (NPPD), identifies risks or requirements to be addressed through BODs. DHS also accepts ideas for potential BODs from entities, such as the Federal Chief Information Officer (CIO) Council, independent security researchers, or other partners. As needed, DHS may convene a group of subject-matter experts from Federal agencies, OMB, and the National Institute of Standards and Technology to consider the relative merits of particular risks in order to determine the appropriateness of a given BOD or determine the prioritization of different BODs.

Generally, when determining whether a certain issue is appropriate for a BOD, DHS considers the following questions:

- Is the proposed BOD related to an active threat? If so, what is the scope and magnitude of the problem?
- Is the proposed BOD related to a potential identified risk?
- What category/schedule does the potential BOD fit into (planned, escalation of issue, or emergency)?
- Is this issue specific to a particular Federal agency or could it be applicable across the civilian Federal Executive branch?
- What is the difficulty to exploit the vulnerability?
- Is the issue/subject Sensitive or Classified?
- Are external events or threat intelligence driving the need for or request of the proposed BOD?
- Can the proposed BOD be measured and validated by DHS?
- Could the issue or threat be addressed satisfactorily and fully through other mechanisms? Has DHS socialized the proposed BOD subject with applicable stakeholders, such as CIO/Chief Information Security Officer (CISO) councils?
- What is the end-state of proposed BOD?
- What other operational requirements have been issued by way of policy, guidance, and standards in relation to this BOD?
- Does the BOD address or re-emphasize Federal program such as CDM, EINSTEIN, automated indicator sharing, etc.?
- Is this BOD associated with the requirements for the content of the annual reports required to be submitted by Federal agencies?
- Is this BOD associated with the requirements for reporting incidents to the NCCIC?

In fiscal years 2015 and 2016, there were four BODs:

BOD 15–01.—In fiscal year 2015, the DHS Secretary issued the first BOD, BOD 15–01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems.* It directs agencies to mitigate critical vulnerabilities discovered by DHS's NCCIC through the NCCIC's scanning of agencies' internet-accessible systems. Mitigation is required within 30 days of notification to the agencies of the vulnerabilities discovered by the NCCIC. DHS assesses the effectiveness of this BOD by monitoring mitigation time lines.

BOD 16–01.—On June 9, 2016, the DHS Secretary issued BOD 16–01, *Securing High-Value Assets,* to require agency participation in risk and vulnerability assessments as well as security architecture reviews conducted by DHS on the high-value assets of agencies. It further requires agencies to mitigate high-priority vulnerabilities discovered during the risk and vulnerability assessments.

Agencies are required to report to DHS the status of mitigating each high-priority vulnerability within 30 days of receiving a high-value asset final assessment report from DHS, and every 30 days thereafter until all high-priority vulnerabilities have been addressed. The status report must state that the vulnerability has been mitigated or explain the constraints preventing mitigation within 30 days and the steps being taken by the agency to achieve mitigation.

BOD 16–02.—On September 27, 2016, the Secretary issued BOD 16–02, *Threat to Network Infrastructure Devices,* to address several urgent vulnerabilities in network infrastructure devices identified in a NCCIC Analysis Report. Specifically, it addressed hacking tools targeting firewalls, Cisco Adaptive Security Appliance, and Cisco ROM Monitor Integrity. Throughout the directive's reporting period, agencies showed progress and actively participated in interagency dialog.

BOD 16–03.—On October 17, 2016, the DHS Secretary issued BOD 16–03, *2016 Agency Cybersecurity Reporting Requirements,* to specify reporting requirements for cyber incidents and the general information security posture of agencies. FISMA re-

quires agencies to report cybersecurity incidents to DHS and to provide annual reports to OMB, DHS, and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. FISMA further requires the DHS Secretary to issue one or more BODs specifying requirements for this reporting.

Question 2a. Under current law, each Federal agency head is responsible for managing cyber risks to their own networks; however, these agencies rely heavily on contractors to carry out programs, activities, and operations.

Does DHS have visibility into how agencies manage the risk of allowing Federal contractors and other individuals from outside the organization to access sensitive data on Government networks?

Question 2b. What more could the Government be doing to mitigate the risk that a virus or other harm will be inflicted unwittingly or purposely by contractors authorized to access Federal networks?

Answer. The Department of Homeland Security (DHS) generally does not have visibility into agency risk-management decisions related to contractor access to information systems. Contractors are subject to the suitability determinations of individual agencies and, more generally, the guidelines included in the Federal Acquisition Regulation. Standardizing the suitability guidelines and raising the security clearance requirements for contractors that have access and/or elevated privileges to sensitive and/or mission-critical systems and data would provide an increased level of assurance of the trust granted to contractors but would not eliminate the risk. At the same time, additional requirements would increase entrance-on-duty wait times.

Question 3. I understand DHS and GSA are currently re-competing the CDM contract, which will expire next years. Is DHS planning to use this opportunity to make improvements to the CDM program and, if so, what are the goals?

Answer. Given the dynamic nature of cybersecurity technology and services, the Department of Homeland Security (DHS) is developing an acquisition approach for the next set of task orders under CDM DEFEND (previously described under the response to Question 5) that will allow for easier execution of contractual actions. DHS expects this approach will streamline responses to agency cyber needs, including the procurement of tools, tool maintenance, and ancillary services. Task orders under CDM DEFEND will be awarded for longer time periods, allowing awardees an opportunity to become familiar with the agency environments associated with the task order. This will enhance an eventual awardee's ability to deliver expanded Continuous Diagnostics and Mitigation (CDM) capabilities from any of the CDM phases. The goal is to provide both the CDM program and agencies a flexible task order that streamlines the ability to deliver CDM functionality based on evolving threats and agency requirements.

Question 4. The acquisition vehicle for CDM, CMaaS (Continuous Monitoring as a Service), was awarded in August 2013. Four years later, Phase 1 of CDM's 4 Phases is still not complete. Given CDM's slow pace, how does DHS expect it to deal with rapidly-evolving cyber threats?

Answer. Continuous Diagnostics and Mitigation (CDM) Phase 1 identified the complexity of network environments within agencies and illustrated the true number of assets connected to agency networks. Overall, this discovery detected 44 percent more assets connected to agency networks than originally identified by agencies. In some cases, agencies had more than 200 percent more assets on their networks than originally identified. By deploying the continuous monitoring tools on agency networks this year, the Federal Government is gaining greater, near-real-time awareness of agency environments than has ever existed.

The under-reporting of assets and understanding of the uniqueness and complexities associated with agency network environments presented real challenges for the CDM program. As a result, changes had to be proposed to Phase 1 procurement agency roll-out schedules to address emerging cyber risks and agency complexities. CDM implementation has also been dependent on limited labor resources of agencies as well as the internal processes of agencies to deploy new technologies. An additional challenge not anticipated was that contractors had to undergo clearance determinations at both DHS and the agency supported.

The program and agencies alike have benefited from this awareness and the lessons learned in working to reduce the complexity. Additionally, as noted in the response to Questions 5 and 17, the next contract vehicle will provide for flexibility and faster deployments if an agency is able to support a faster pace. The program will forego the time and expense of establishing a replacement BPA, and instead leverage efficiencies established under GSA's Alliant GWAC for CDM DEFEND.

Question 5. We all know what the bad guys seek to do: Steal or, perhaps worse, alter data. Data Protection capabilities do not get rolled out until Phase 4 of CDM. At the current pace, it could be 10 years before CDM completes Phase 4. What ef-

forts, if any, are under way to accelerate reaching the Data Protection Phase of CDM?

Answer. The President's fiscal year 2017 budget request included funding for a newly-proposed Continuous Diagnostics and Mitigation (CDM) Phase 4 to expand the CDM program to include additional tools and services to protect sensitive and high-value asset data within agency networks. While not fully funding the requested level, the fiscal year 2017 Consolidated Appropriations Act provided funds to begin the planning activities necessary to define CDM Phase 4 in preparation for an acquisition review in late fiscal year 2018.

There are fundamental technical steps that have to be in place prior to focusing on the data, such as identifying the assurance level on the user's identity and the degree of hardening and protections within the infrastructure that holds the data. This is done through the implementation of key parts of Phases 1, 2, and 3.

The CDM program and its customer agencies have devoted the last 2 years to building out the foundation for all cybersecurity work. Addressing the "what is on the network" (Phase 1) and "who is on the network" (Phase 2) are issues that had been challenging agencies for more than a decade. CDM has made significant progress in the resolution of these key capabilities over the past 2 years and can continue to build on this for "what is happening on the network" (Phase 3) and Phase 4 "protecting data on the network" (Phase 4).

Question 6. In light of how rapidly cybersecurity tools are developed and rolled out, is it possible that the tools being offered in Phase 1 are already obsolete? What is the mechanism for refreshing Phase 1 tools?

Answer. The tools provided through Phase 1 of Continuous Diagnostics and Mitigation (CDM) offer current technology that is critical to providing the fundamental real-time awareness of what is on agency networks. The existing mechanism for adding approved products will continue to ensure that the approved product list is able to respond to the evolving marketplace. The program plans to continue using an Approved Products List (APL). The program will only consider products that have been placed on GSA's Information Technology (IT) Schedule 70 contracts. The program will perform both conformance and technical reviews prior to approval. Once approved, vendors will have the opportunity to submit the product for inclusion on the GSA's newly-created CDM Special Item Number (SIN), which will provide a contract solution to maintain and then expand the CDM Product catalog. Open season periods (available to all GSA IT Schedule holders) will be held each month to allow for timely refresh. CDM is based on procuring innovative, commercial-off-the-shelf products. It is important, however, to be mindful of challenges related to product maturity, as the CDM program does not want to deploy products that have not been rigorously coded and tested. Products cannot be added to the CDM SIN unless a product has been approved by the Program and added to the APL. Initially, the APL will consist of all CDM products that have been evaluated and approved on the CMaaS BPA. New products will be continually added to the APL through a DHS evaluation process that standardizes the evaluation of products to ensure conformance with DHS developed criteria. While the DHS PMO will manage the APL, the CDM SIN (contract administration and execution) will be managed by the GSA IT Schedule 70 program office.

Question 7. We have heard of situations where an agency buys a cybersecurity tool but never deploys it, commonly referred to as "shelfware." What options has DHS considered for dealing with this problem throughout the Federal Government and within its own components? Are there vehicles—for instance, a CDM Task Order calling on prime contractors to integrate shelfware—DHS could use to expedite the deployment of much-needed cyber tools?

Answer. Agencies can consult with the Department of Homeland Security regarding whether an existing tool, deployed or not, meets Continuous Diagnostics and Mitigation (CDM) program requirements. CDM publishes a product catalog through the General Services Administration (GSA), available on-line, that identifies CDM-approved tools. The CDM program has provided labor support to agencies who reported they already had existing products but did not have them deployed. Since these products were part of the CDM solution, it was deemed in the best interest of the Government to ensure they did not remain "shelfware." In future phases, CDM will continue to maintain approved product lists that crosswalk CDM-approved tools to CDM capabilities. Additionally, CDM will offer contract vehicles that agencies can use to fund installation, configuration, and integration activities associated with existing products already procured by agencies that remain compliant with CDM requirements.

Question 8. From your vantage point, what are the benefits of utilizing the acquisition innovation approaches, as developed by DHS's Office of Procurement, for cybersecurity acquisitions?

Answer. The Department of Homeland Security (DHS) is leveraging new, innovative approaches for cybersecurity acquisitions. For instance, DHS's Procurement Innovation Lab was used to acquire the EINSTEIN 3 Accelerated Service Extension contract. This contact was awarded in record time with a significant negotiated reduction in cost for the service.

Question 9a. As we learned from the 2015 OPM breach, a successful intrusion against a Federal network may compromise sensitive data stored in the recent past as well as data that is several years old. In fact, many of the victims of the OPM breach had not worked for the Federal Government in over a decade.

When a DHS employee leaves his or her position, what processes does DHS follow to ensure that Sensitive but Non-classified information is protected on that former employees' computer hard drive, cell phone, badge, and other electronic media?

Answer. Each component is responsible for handling their own check-out processing. DHS Headquarters (HQ) has an out-processing checklist for personnel to follow. This includes reminders to turn in cell phones, laptops, badges, travel cards, etc. For example:

- *Computer hard drive*.—Laptop, desktop, and tablet computers issued by HQ are asset-tagged items and require the return of the item when a user departs. DHS HQ rewrites the computer hard disk drive (HDD) during the imaging process for computers being reutilized. For computers being decommissioned, the HDD is removed and shredded by an authorized recycler.
- *Cell phone*.—For all DHS HQ departing users, the cell phone is retrieved and either factory wiped for reuse or it is recycled whereby the phone is destroyed by an authorized recycler.
- *Other electronic media*:
  - *External HDD*.—External HDDs issued by DHS OCIO are asset-tagged items and require the return of the item when a user departs. DHS OCIO wipes the external HDD if the password is provided, if no password is provided the external HDD is shredded by an authorized recycler.

Question 9b. To what extent does DHS promote the adoption of cloud services, minimizing the amount of data stored on Federal servers, and proper destruction of hard drives?

Answer. DHS promotes the adoption of cloud services, for data storage and processing. For instance, DHS is planning to adopt cloud email, and DHS components have already migrated some information systems into the cloud. While some specialized applications may need to continue to remain on servers and hardened systems located in Federal facilities, DHS and its components should be able to use cloud storage to minimize the amount of data stored on Federal servers. DHS will continue its current practice of properly destroying hard drives once they are no longer needed.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR JEANETTE MANFRA

Question 1a. In your written testimony, you note that the Cybersecurity Act of 2015 required the application of available EINSTEIN protections to all information traveling to or from Federal information systems by December 2016. While the percentage of traffic that is monitored has increased significantly, full protection has not yet been achieved.

What obstacles has NPPD encountered in achieving a full implementation of this system across all agencies?

Question 1b. How will NPPD address them?

Question 1c. What is the Department's plan for protecting networks with E3A that are not served by traditional internet service providers?

Answer. The Cybersecurity Act of 2015 directs Federal agencies to apply and continue to utilize the intrusion detection and prevention capabilities made available by the Department of Homeland Security (DHS) to all information traveling between an agency information system and any information system other than an agency information system. These intrusion detection and prevention capabilities made available by DHS are known as EINSTEIN.

Agencies have made significant progress in applying and continuing to utilize available EINSTEIN protections since the passage of the Cybersecurity Act of 2015. Prior to passage of the Act, EINSTEIN 3A protections covered approximately 38 percent of Federal civilian users. Today, at least one of the EINSTEIN 3A protections are being utilized by over 90 percent of the Executive branch civilian workforce. This progress was also supported by engagement from DHS leadership. In May 2016, the DHS Secretary sent a letter sent to his peers at the largest agencies requesting their full participation in EINSTEIN consistent with the requirements in law. DHS continues to work with all remaining Federal civilian agencies to facili-

tate their full participation in EINSTEIN. At the same time, DHS is developing new capabilities and conducting a strategic review of the program architecture in order to provide even more protections for Federal agencies.

While considerable progress has been made since the passage of legislation by Congress, there have been some obstacles to achieving full implementation. For instance, due to unique network architectures, autonomous components, and variations in internet service providers (ISPs), large agencies took several weeks or months to fully on-board all components. At the smaller agencies, while smaller network footprints and the wide-spread use of managed trusted internet protocol service make deployment easier, staff resources are limited and deployment competes with their day-to-day operational requirements and other cybersecurity initiatives. Among the smaller agencies, DHS prioritized those that have been proactive and responsive as well as those with regulatory and mission-critical responsibilities. Agencies use different ISPs, with various levels of experience on-boarding agencies, causing a delay for some. Finally, there were technical challenges with accommodating a large and diverse customer set with unique network infrastructure and technical concerns, such as Internet Protocol version 6 and Domain Name System Security Extensions capabilities, lack of consolidated Domain Name System, and outdated infrastructure. Many agencies use third-party, cloud-based email services. DHS may not be able to provision email filtering service for all of those agencies due to a number of technical challenges; however, work continues with the agencies and their service providers to engineer solutions. DHS continues to work closely with agencies to resolve technical challenges that arise during deployment of EINSTEIN capabilities.

DHS has contracts with three major ISPs to provide EINSTEIN services to Federal civilian Executive branch agencies. In some cases, agencies receive service from an ISP other than one of those major three. In such cases, DHS competitively awarded a contract to an ISP that allows those agencies to route their traffic through a capability that allows them to receive protections as well. This contract and service is referred to as EINSTEIN 3A Service Extension.

Question 2a. The DHS Continuous Diagnostic and Mitigation program is a step in the right direction to identify the devices and software on our Federal networks and to enable timely corrective action.

What metrics has your organization identified for assessing the effectiveness of these measures?

Question 2b. By what evidence were they selected?

Question 2c. With respect to CDM Phase IV:

What are the goals of Phase IV?

How were those goals selected?

What is the status of Phase IV implementation?

What is the time line for deployment of Phase IV technologies across the .gov domain?

Answer. The success of the Continuous Diagnostics and Mitigation (CDM) program will be assessed against several criteria, including the extent to which Federal agencies use CDM tools, including the Federal and agency-level dashboards, to prioritize cybersecurity risks and fix the most significant vulnerabilities first. Additionally, CDM is looking to achieve a measurable reduction of both the prevalence and severity of cybersecurity incidents across Government networks, as a result of the CDM tools deployed. The CDM program is refining how success is measured and working to define a series of mission outcome metrics to measure the impact and effectiveness of the program.

The first of these metrics is simply gaining a better understanding of the total number of assets, or the overall cyber attack surface, in agency network environments. Through the discovery process of CDM Phase 1, there was an overall approximate 44 percent increase in the total number of assets on agency networks compared to what agencies had previously known through manual tracking. In some agencies, the assets identified were more than 200 percent greater than initially reported.

As CDM tools and technologies are deployed and integrated into the agency network environments, the agencies will be able to baseline their initial vulnerability and configuration cybersecurity posture through their agency dashboard. Likewise, the Federal dashboard will display cybersecurity posture across the agencies. From that baseline, agencies and DHS will be able to measure improvements in vulnerability patching and configuration hardening across the agencies. Already, DHS has witnessed multiple examples of agencies prioritizing the patching of critical and high-priority vulnerabilities as they gain better visibility of their networks with CDM tools. Based on the experience of agencies with strong continuous monitoring programs, agency cyber hygiene should improve significantly.

DHS currently measures success of the CDM program through collection and analysis of agency FISMA submissions. CDM's deployment of Phase 1 tools resulted in noticeable improvement in performance measures associated with hardware and software asset management, configuration management, as well as vulnerability and patch management. DHS will continue to measure effectiveness of CDM efforts through continued collection and analysis of FISMA CIO and IG performance measures.

CDM tools, other DHS capabilities, and risk management will help agencies Identify, Protect, Detect, Respond, and Recover to cyber threats. Already, the CDM program is working to develop measures of system importance to capture a better understanding of the protections in place for mission-essential and high-value systems. This measure of impact, along with metrics for addressing boundary protections and data protections on mobile devices and in the cloud, will allow the Federal Government to continue to improve at measuring its cybersecurity risk in real time. These efforts are informed by risk-scoring research done by NIST, prior risk-scoring frameworks used by the agencies, and industry risk-scoring approaches.

The President's fiscal year 2017 budget request included funding for a newly-proposed Continuous Diagnostics and Mitigation (CDM) Phase 4 to expand the CDM program to include additional tools and services to protect sensitive and high-value asset data within agency networks. While not fully funding the requested level, the fiscal year 2017 Consolidated Appropriations Act provided funds to begin the planning activities necessary to define CDM Phase 4 in preparation for an acquisition review in late fiscal year 2018.

There are fundamental technical steps that have to be in place prior to focusing on the data, such as identifying the assurance level on the user's identity and the degree of hardening and protections within the infrastructure that holds the data. This is done through the implementation of key parts of Phases 1, 2, and 3.

Question 3a. During your testimony, you noted that two of the Binding Operational Directives (BODs) were closed and two remain open to continuing measuring their effectiveness.

What were the closure criteria for BOD–16–02 and BOD–16–03?

When did each agency meet those criteria?

When were the BODs closed?

What is the current percentage of critical vulnerabilities that remain unmitigated? What percentage of critical vulnerabilities were left in place with a justification?

Question 3b. What is the current state of implementation of BOD–15–01 and BOD–16–01?

Question 3c. With respect to implementing all of the BODs:

What are the most and least responsive agencies?

What is the average time for compliance?

Answer. The Secretary of Homeland Security (DHS), in consultation with the director of the Office of Management and Budget, has the authority to develop and oversee the implementation of binding operational directives (BODs). The statute includes specific topics for BODs, including requirements for reporting security incidents to DHS's National Cybersecurity and Communications Integration Center (NCCIC), requirements for the contents of the annual Federal Information Security Modernization Act (FISMA) reports, requirements for the mitigation of exigent risks to information systems, and other operational requirements as the Office of Management and Budget (OMB) or DHS, in consultation with OMB, may determine necessary.

In fiscal years 2015 and 2016, there were four binding operational directives:

BOD 15–01.—In fiscal year 2015, the Secretary issued the first BOD, BOD 15–01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems.* It directs agencies to mitigate critical vulnerabilities discovered by DHS's National Cybersecurity and Communications Integration Center (NCCIC) through the NCCIC's scanning of agencies' internet-accessible systems. Mitigation is required within 30 days of notification to the agencies of the vulnerabilities discovered by the NCCIC. DHS assesses the effectiveness of this BOD by monitoring mitigation time lines. This BOD will remain open given that vulnerability scanning occurs regularly and is on-going.

BOD 16–01.—On June 9, 2016, the Secretary issued BOD 16–01, *Securing High-Value Assets,* to require agency participation in risk and vulnerability assessments as well as security architecture assessments conducted by DHS on agencies' high-value assets. It further requires agencies to mitigate high-priority vulnerabilities discovered during the risk and vulnerability assessments.

Agencies are required to report to DHS the status of mitigating each high-priority vulnerability within 30 days of receiving a high-value asset final assessment report

from DHS, and every 30 days thereafter until all high-priority vulnerabilities have been addressed. The status report must state that the vulnerability has been mitigated or explain the constraints preventing mitigation within 30 days and the steps being taken by the agency to achieve mitigation. This BOD will remain open given ongoing assessments of high-value assets.

BOD 16–02.—On September 27, 2016, the Secretary issued, BOD 16–02, *Threat to Network Infrastructure Devices,* to address several urgent vulnerabilities in network infrastructure devices identified in a NCCIC Analysis Report. Specifically, it addressed hacking tools targeting firewalls, Cisco Adaptive Security Appliance, and Cisco ROM Monitor Integrity. Throughout the directive's reporting period, agencies showed progress and actively participated in interagency dialog.

BOD 16–02 required all Federal agencies to perform actions specified in the NCCIC's Analysis Report within 45 days, to report full mitigation or a detailed plan of action and milestones, and to provide monthly updates until full mitigation is achieved. Federal agencies promptly began taking action by implementing solutions or compensating controls, and reporting to DHS on a monthly basis. Though not all agencies have fully mitigated certain vulnerabilities, all have made significant progress and are reporting status and constraints to DHS as required. At this time, a very small percentage of potentially impacted devices have yet to be reported by the agencies as fully mitigated.

BOD 16–03.—On October 17, 2016, the Secretary issued, BOD 16–03, *2016 Agency Cybersecurity Reporting Requirements,* to specify reporting requirements for cyber incidents and the general information security posture of agencies. The Federal Information Security Management Act of 2014 (FISMA) requires agencies to report cybersecurity incidents to DHS and to provide annual reports to OMB, DHS, and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. FISMA further requires the Secretary to issue one or more BODs specifying requirements for this reporting. Federal agencies coordinated with DHS to prepare for the updates to the Federal Incident Notification guideline changes. The directives in this BOD remain in effect for the remainder of fiscal year 2017.

Regarding the responsiveness of agencies to requirements of BODs, all agencies are compliant with the communication requirements and are responsive to DHS requests for information. Agencies have been making steady progress toward mitigating vulnerabilities and working to fulfill the requirements of the BODs. In some cases, certain network and system constraints have been affecting the time frame for fulfilling requirements in BODs. Agencies have been working through such constraints by implementing compensating controls or are working with their leadership to determine long-term solutions while reporting status to DHS per the requirements in the BODs. In general, most agencies have been able to mitigate identified vulnerabilities within the initial time frames mandated by specific BODs. For the remaining agencies, all have provided regular updates and are in contact with the DHS team as they continue to close out remaining actions.

Question 4a. With respect to the issuance of BODs:

Which office(s) generates proposals for BODs?

Question 4b. What criteria are applied to determine whether a BOD should be issued?

Question 4c. What criteria are applied to determine when a BOD should be issued?

Question 4d. Is there any interagency consultation before a BOD is issued? What is the nature of the consultation, if it exists?

Question 4e. Does the Secretary consult with the Office of Management and Budget before issuing a BOD? Any other component of the Executive Office of the President?

Question 4f. Has the idea for a BOD ever originated outside of the Department of Homeland Security?

Answer. The Secretary of Homeland Security (DHS), in consultation with the director of the Office of Management and Budget, has the authority to develop and oversee the implementation of binding operational directives (BODs). The statute includes specific topics for BODs, including requirements for reporting security incidents to DHS's National Cybersecurity and Communications Integration Center (NCCIC), requirements for the contents of the annual Federal Information Security Modernization Act (FISMA) reports, requirements for the mitigation of exigent risks to information systems, and other operational requirements as the Office of Management and Budget (OMB) or DHS, in consultation with OMB, may determine necessary.

DHS, acting through the National Protection and Programs Directorate, identifies risks or requirements to be addressed through BODs. DHS also accepts ideas for potential BODs from entities, such as the Federal Chief Information Officer (CIO)

Council, independent security researchers, or other partners. As needed, DHS may convene a group of subject-matter experts from Federal agencies, OMB, and the National Institute of Standards and Technology (NIST) to consider the relative merits of particular risks in order to determine the appropriateness of a given BOD or determine the prioritization of different BODs.

Generally, when determining whether a certain issue is appropriate for a BOD, DHS considers the following questions:

- Is the proposed BOD related to an active threat? If so, what is the scope and magnitude of the problem?
- Is the proposed BOD related to a potential identified risk?
- What category/schedule does the potential BOD fit into (planned, escalation of issue, or emergency)?
- Is this issue specific to a particular Federal agency or could it be applicable across the civilian Federal Executive branch?
- What is the difficulty to exploit the vulnerability?
- Is the issue/subject Sensitive or Classified?
- Are external events or threat intelligence driving the need for or request of the proposed BOD?
- Can the proposed BOD be measured and validated by DHS?
- Could the issue or threat be addressed satisfactorily and fully through other mechanisms?
- Has DHS socialized the proposed BOD subject with applicable stakeholders, such as CIO/Chief Information Security Officer (CISO) councils?
- What is the end-state of proposed BOD?
- What other operational requirements have been issued by way of policy, guidance, and standards in relation to this BOD?
- Does the BOD address or re-emphasize Federal programs such as CDM, EINSTEIN, automated indicator sharing (AIS), etc.?
- Is this BOD associated with the requirements for the content of the annual reports required to be submitted by Federal agencies?
- Is this BOD associated with the requirements for reporting incidents to the NCCIC?

QUESTIONS FROM HONORABLE VAL DEMINGS FOR JEANETTE MANFRA

Question 1. What actions is DHS taking to advance the implementation of CDM tools and capabilities at Federal agencies?

In particular, is the Department providing technical training to agency system administrators on the use of the CDM tools so they know how to effectively and optimally use the tools to diagnose and mitigate vulnerabilities?

Answer. The Continuous Diagnostics and Mitigation (CDM) program anticipated training requirements for operation and management of capabilities. Training requirements were included in the contract solicitation. All CDM integrators are required to provide sufficient training to enable agencies to transition the CDM tools to agency operation once the integrator contract is completed.

Funds available for training are limited, and experience is showing that agencies are requesting more detailed, sustained training options. As such, one area where additional training is under development is for the use of the agency dashboard. CDM is developing on-line, hands-on workshops in fiscal year 2017 to assist agencies with understanding how to use the CDM agency dashboard. It should be noted that CDM program-funded training is intended to get agencies transitioned from CDM tool implementation to agency operations. Cybersecurity operations and sustainment is ultimately the responsibility of each agency, and it is the agency's responsibility to engage with DHS to fully utilize available resources.

Question 2. What feedback mechanism does DHS have for soliciting and receiving comments from agencies on their experience with the CDM program?

Based on that feedback, what benefits and challenges have the agencies identified with the program?

Answer. During the summer of 2016, the Federal Chief Information Officer (CIO) held a CyberStat on the Continuous Diagnostics and Mitigation (CDM) program. The CyberStat included program documentation review, interviews conducted by Office of Management and Budget (OMB) staff with several agencies, and meetings between the Federal CIO and the CIO or Chief Information Security Officer (CISO) of each agency. This CyberStat was a valuable source of feedback. The Federal CIO noted that "all participants expressed support for the security objectives of the program and emphasized their commitment to procuring CDM Phase 1 tools."

Other benefits included:

- Establishing a consistent approach toward information security continuous monitoring of networks across the Federal civilian agency enterprise. The Federal Information Security Management Act FISMA of 2002 requires agencies to provide security for the networks that support the operations and assets of their agency. The Federal Information Security Modernization Act of 2014 reiterates those requirements and codifies the Department of Homeland Security's (DHS) authority, in consultation with OMB, to administer the implementation of information security policies and practices for civilian agencies. Through CDM, agencies receive a significant investment by DHS to boost previous efforts and, in many instances, are able to achieve an internally consistent enterprise approach, allowing them to leverage similar product knowledge, subject-matter expertise, and technical support across the agency.
- Pioneering an innovative acquisition approach by combining agencies into groups for similar requirements and project efficiencies. By grouping agencies, CDM is achieving economies of scale and reducing pricing for labor and products. To date, CDM has achieved cost avoidance of $600 million on products over the Schedule 70 pricing.
- Leveraging a consistent system engineering life cycle, tailored from DHS.
- Establishing an approach toward supply chain risk management across the Federal civilian Government enterprise. To date, the program has applied secure delivery controls for well over 1 million products delivered to participating agencies.

Challenges identified by some agencies included issues such as: Asset and infrastructure gaps, agency governance and management challenges, integrator project management challenges, training and knowledge management, entrance on duty requirements, and selection of tools and requirements. With regard to the identified gaps, agencies noted that CDM revealed a significant number of new end-points, and unplanned infrastructure upgrades and modernization may be required to support new CDM tool deployments. These activities resulted in budget implications for agencies. Further, since additional end-points were identified, future-year license maintenance costs will increase, adding additional pressure to future budgets. Governance challenges include the need for CIO engagement and leadership with clear project management. Integrator project management challenges were identified as requiring proactive engagement and communications with the agencies, and well-documented plans, schedules, etc. The program worked closely with each integrator to ensure plans and schedules were clearly communicated on a timely basis.

The CDM program office has worked with OMB on the next steps, including implementing improvements and addressing concerns, as appropriate. Moving forward, CDM has established a Customer Advisory Forum (CAF) comprised of CISOs, or designees, from each agency in order to receive feedback on topics of interest and concern. The CAF will continue to meet on a bi-monthly basis and will serve as the focal point for interagency collaboration related to CDM planning and implementation, including customer proposals and adoption, organizational and technical challenges, acquisition planning, and capability integration priorities.

Question 3a. GAO made nine recommendations in January 2016 to DHS to enhance the functionality of the EINSTEIN program.

What is the status of DHS efforts to implement those recommendations?

Question 3b. When does the Department expect to fully implement them?

Answer. The nine recommendations made by the Government Accountability Office (GAO) and a status update for each are provided below.

Recommendation 1.—"NSD [Network Security Deployment] to determine the feasibility of enhancing NCPS's [National Cybersecurity Protection System's] current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines."

The Department of Homeland Security (DHS) concurred with this recommendation. DHS acknowledges that it must rapidly identify, pilot, and deploy new technologies and solutions that effectively detect and block previously unknown threats. DHS continues to conduct an anomalous analytics capability that directly addresses the recommendation to "detect deviations from normal network behavior baselines." DHS has determined that the technology and architectural approach to deploying such a capability within the NCPS is feasible. In order to operationalize this pilot capability and deliver a production version, additional contract resources are required.

Recommendation 2.—"NSD to determine the feasibility of developing enhancements to current intrusion detection capabilities to facilitate the scanning of encrypted, SCADA, and IPv6 traffic."

DHS concurred with this recommendation. DHS has been conducting an analysis on Security on Encrypted Traffic (SonET) to better understand options for address-

ing the challenges of encrypted traffic and engaging with the broader standards community to ensure this is being addressed at a broader industry level. The SonET analysis study is on-going and expected to last through the fourth quarter of fiscal year 2017.

DHS continues to discuss SCADA traffic with its ICS–CERT to get a better understanding of SCADA traffic that passes through network gateways. These discussions remain on-going.

NCPS intrusion detection (EINSTEIN 1 and EINSTEIN 2) sensors are capable of scanning Internet Protocol version six (IPv6) traffic. The NCPS program is continuing to work with the internet service providers (ISPs) providing NCPS intrusion prevention (EINSTEIN 3) capabilities as they finalize their plans to fully support IPv6. An implementation plan that would address all ISP schedules is expected in the third quarter of fiscal year 7.

Recommendation 3.—"US–CERT to update the tool it uses to manage and deploy intrusion detection signatures to include the ability to more clearly link signatures to publicly-available, open-source data repositories."

DHS concurred with this recommendation. DHS developed a capability to meet the spirit of this recommendation, and GAO is working to formally close out this recommendation.

Recommendation 4.—"US–CERT to consider the viability of using vulnerability information, such as data from the Continuous Diagnostics and Mitigation program as it becomes available, as an input into the development and management of intrusion detection signatures."

DHS concurred with this recommendation. The data available from the Continuous Diagnostics and Mitigation (CDM) program will be directly relevant to prioritization of signatures. The CDM collection sensors will allow analysts to view software vulnerabilities correlated with deployments at specific agencies. Based on this information, DHS may prioritize signature development based on known exposure rates at an agency to detect instances of intrusions and when possible to block intrusions. The CDM data may be combined with known vulnerability findings from DHS's National Cybersecurity and Communications Integration Center (NCCIC) and known threats to further prioritize signature development, as necessary. The overall signature development process and prioritization needs to take into account victim exposure, threat prevalence, and criticality of vulnerabilities in managing risk. The data will be viable once CDM is operational and reporting to the Federal dashboards. As additional CDM data becomes available, DHS will work with GAO to close out this recommendation.

Recommendation 5.—"US–CERT to develop a time table for finalizing the incident notification process, to ensure that customer agencies are being sent notifications of potential incidents, which clearly solicit feedback on the usefulness and timeliness of the notification."

DHS concurred with this recommendation. DHS regularly solicits feedback from Federal agencies on the timeliness and usefulness of incident reporting. To better support feedback and data quality from Federal agencies, DHS, in coordination with the Office of Management and Budget (OMB), has completed updates to the Incident Reporting Guidelines in order to resolve previously-mentioned process concerns. New data quality activities are now in place as of January 2017. Additional updates are under development to add a feature change for user feedback following incident ticket closure. This feature is expected to be implemented by October 2017.

Recommendation 6.—"The Office of Cybersecurity and Communications (CS&C) to develop metrics that clearly measure the effectiveness of NCPS's efforts, including the quality, efficiency, and accuracy of supporting actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information."

DHS concurred with this recommendation. In general, cybersecurity metrics remain an area of active research in both Government and industry, and DHS is exploring opportunities to engage with the research community as well. DHS continues to develop metrics. Several output and outcome metrics have been identified. The NCCIC is continuing to baseline one of the measures related to EINSTEIN 3 Accelerated for a possible fiscal year addition to the Government Performance and Results Act set of measures.

DHS is working to develop a second set of measures focused on information sharing. As part of its customer feedback process, DHS is exploring how its public and private-sector recipients of information measure the value of cyber threat indicators and defensive measures. Work on this response is on-going.

Recommendation 7.—"CS&C to develop clearly-defined requirements for detecting threats on agency internal networks and at cloud service providers to help better ensure effective support of information security activities."

DHS concurred with this recommendation. This recommendation will be in large part addressed by Continuous Diagnostics and Mitigation (CDM) Phase 3, which will provide agencies with tools to help them understand what is happening on their network and identify anomalous activity. However, DHS's responsibility in Federal cybersecurity is inherently limited by law and policy. Each agency retains responsibility for implementing an effective defense-in-depth strategy to protect their networks. To this end, DHS requires each agency's consent prior to providing any cybersecurity assistance or services, including CDM and EINSTEIN.

Recommendation 8.—"NSD to develop processes and procedures for using vulnerability information, such as data from the CDM program as it becomes available, to help ensure DHS is using a risk-based approach for the selection/development of future NCPS intrusion prevention capabilities."

DHS concurred with this recommendation. As CDM is focused on monitoring the internal assets of an agency's network and NCPS's EINSTEIN is positioned on the external network boundary, combining data from both programs will allow DHS to understand potentially malicious activity that cannot be understood by either program in isolation. As CDM data becomes available, DHS will correlate data from EINSTEIN and CDM to enhance NCPS's EINSTEIN capabilities, either by enriching indicators or by identifying future intrusion prevention capabilities. In preparation of future integration efforts, DHS continues to enhance the data correlation model of NCPS and CDM. Work is expected to continue in fiscal year and will be enhanced as more data becomes available from the CDM program.

Recommendation 9.—"NSD to work with their customer agencies and the internet service providers to document secure routing requirements in order to better ensure the complete, safe, and effective routing of information to NCPS sensors."

DHS concurred with this recommendation. DHS has been collaborating with the Federal agencies to address their challenges with routing traffic through their Trusted Internet Connection (TIC) gateways, to include development of alternative approaches for routing Government network traffic more efficiently, while maintaining the DHS-required situational awareness. The DHS TIC program has been working closely with OMB to develop a TIC Action Plan outlining the activities and objectives to develop the next generation TIC Reference Architecture. This document will serve as the new guidance for agencies on perimeter security capabilities as well as alternative routing strategies. It is expected that all Federal agencies will be invited to participate in this effort, providing feedback on their challenges. At the conclusion of this effort, OMB will update policy to align with the new TIC Reference Architecture.

OMB has also been working in parallel on developing cloud policies. A Security Architecture Tiger Team consists of agency stakeholders, including DHS, to develop a broader security strategy for agency cloud adoption. The expectation is that the TIC and cloud policies would be aligned. In addition, DHS is working to incorporate the alternative routing strategies approaches into its future technical roadmap.

Also of note, DHS has been working closely with the General Services Administration (GSA) on incorporating cybersecurity requirements into the next generation GSA EIS contract (formerly referred to as Networx 2020). Agencies will use this contract to procure internet and telecommunications services. By baking in security requirements for internet service providers and telecommunications carriers, it should reduce the re-engineering and design efforts currently burdening the agencies. The second round of evaluations is currently under way.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR GREGORY C. WILSHUSEN

Question 1. At the hearing we discussed DHS's NCPS and CDM programs. What other actions can DHS take to assist Federal agencies with protecting their information and information systems?

Answer. DHS can enhance or expand its capabilities to share information on cyber threats with Federal agencies. As we reported in May 2016, 15 of 18 Federal agencies that we surveyed indicated that a lack of Government-wide information-sharing mechanisms limited their ability to identify cyber threats to a great or moderate extent.[1] DHS, in its role as the Federal civilian interface for sharing cyber threat indicators and cybersecurity risks among Federal and non-Federal entities, manages the

[1] GAO, *Information Security: Agencies Need to Improve Controls Over Selected High-Impact Systems,* GAO–16–501 (Washington, DC: May 2016). The 18 agencies we surveyed were those departments and agencies covered by the Chief Financial Officers Act that also reported having high-impact systems. High-impact systems are those for which the agency has determined that the loss of the confidentiality, integrity, or availability of the information or information system could result in severe or catastrophic harm to the organization's operations, assets, or personnel.

Automated Indicator Sharing program which was created to provide real-time sharing of cyber threat indicators and defensive measures. As we reported in February 2017, DHS officials stated that seven Federal agencies were connected to the program as of August 2016.[2] Expanding this program to all 24 Federal agencies covered by the *Chief Financial Officers Act,*[3] which DHS officials said they were doing, could improve the cyber threat information available to those agencies.

DHS can also issue binding operational directives that require agencies to take specific actions to safeguard Federal systems and information from a known or reasonably-suspected information security threat, vulnerability, or risk. The *Federal Information Security Modernization Act of 2014 (FISMA)*[4] authorizes the Secretary of Homeland Security to administer the implementation of agency information security policies and practices for information systems, including developing and overseeing the implementation of binding operational directives. The directives are compulsory directions to an agency to implement policies, standards, and guidelines developed by the Director of the Office of Management and Budget and can include requirements for the mitigation of exigent risks to information systems. As of March 2017, 27 months after receiving this authority, DHS has issued four directives.

In addition, DHS can provide operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security by developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the agencies' information systems. Authorized by FISMA, these assessments can provide agencies with information on how to harden their security and identify the signs that an attacker is on their network.

Further, DHS can continue to participate in *CyberStat* reviews. As explained in my written testimony statement, these reviews are in-depth sessions with National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration. According to OMB, these interviews are face-to-face, evidence-based meetings intended to ensure that agencies are accountable for their cybersecurity posture. The sessions are to assist the agencies in developing focused strategies for improving their information security posture in areas where there are challenges.[5]

Question 2. What does DHS need to consider to ensure CDM objectives and requirements keep pace with the rapidly-evolving nature of cyber threats?

Answer. DHS needs to consider the adaptability and flexibility of the tools and services it offers to agencies under the CDM program. The program is to provide agencies with the tools and services to identify cybersecurity risks on an on-going basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. CDM tools include sensors that perform automated searches for known cybersecurity vulnerabilities, the results of which can feed into a dashboard that alerts network managers. Because of the rapidly-evolving nature of cyber threats and the continual discovery of new vulnerabilities in information systems, DHS needs to ensure that CDM tools can be refreshed or updated on a regular basis to reflect the current state of cyber threats and vulnerabilities. Associated with this capability is the need to ensure that there is a mechanism for delivering system updates to the tools that have been deployed at Federal agencies.

In addition, as we recommended in January 2016, DHS should consider the viability of using vulnerability data garnered through the CDM program as it becomes available as an input into the development and management of intrusion detection signatures for the EINSTEIN intrusion detection/intrusion prevention system. DHS concurred with our recommendation and indicated that it was working to implement this recommendation.

Question 3. One of the priorities of this committee is to ensure the Federal Government is effectively leveraging innovative cybersecurity technologies. The private sector today is able to readily leverage the latest security services through commer-

---

[2] GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely,* GAO–17–163 (Washington, DC: February 2017).

[3] The 24 departments and agencies covered by the Chief Financial Officers Act are 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 U.S. Agency for International Development.

[4] (Pub. L. No. 113–283, Dec. 18, 2014).

[5] GAO, *Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems,* GAO–17–518T (Washington, DC: March 2017).

cial cloud capabilities. What role should DHS play in helping Federal agencies consider and potentially migrate to the cloud?

Answer. As one of three members of the Federal Risk and Authorization Management Program's (FedRAMP)[6] Joint Authorization Board, the DHS Chief Information Officer (CIO) plays a key role in helping Federal agencies consider and potentially migrate to the cloud. The board defines and establishes the FedRAMP baseline system security controls and the accreditation criteria for third-party assessment organizations. The DHS CIO and other board members help ensure that baseline security controls are incorporated into consistent and repeatable processes for security assessment and authorizations of cloud service providers. In this way, the DHS CIO helps agencies achieve a level of assurance regarding the security controls implemented by cloud service providers that receive a board provisional authority to operate.

In addition, DHS can assist agency migration to the cloud by:

- assisting Government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity;
- coordinating cybersecurity operations and incident response;
- developing continuous monitoring guidelines for on-going cybersecurity of Federal information systems; and
- developing guidance on agency implementation of the Trusted Internet Connection program [7] with cloud services.

QUESTIONS FROM HONORABLE JAMES LANGEVIN FOR GREGORY C. WILSHUSEN

Question 1. In your written testimony you spoke to the challenges that DHS has in securing and defending the .gov domain.

Are these issues driven by a lack of authority, resources, or execution?

Answer. DHS efforts in securing and defending the .gov domain have been hampered, in part, by execution shortfalls. For example, as we reported in January 2016, DHS's National Cybersecurity Protection System (NCPS) was partially, but not fully, meeting its stated objectives. The system's ability to detect potentially malicious activity entering or exiting computer networks at Federal agencies was limited because DHS did not design the system to: (1) Monitor all types of network traffic, (2) detect variations from pre-defined baselines of normal network activity, or (3) detect malicious traffic that exploits many common security vulnerabilities.

In addition, the Department had not implemented an effective information-sharing mechanism for alerting agencies to potentially malicious traffic entering their networks or for receiving feedback on the usefulness of the alerts. DHS also had not developed or provided guidance to agencies on how to route network traffic securely through the NCPS's sensors, resulting in some network traffic bypassing the sensors. As a result of these execution shortfalls, DHS had limited assurance that the system could be effective in securing and defending the .gov domain.

Question 2. What executive or legislative measures can be taken to ensure that we have adequate talent within the Government to address the increasing cyber threat?

Answer. Several Executive branch initiatives have been launched and Federal laws enacted that address the Federal cybersecurity workforce. For example, in July 2016, the Office of Personnel Management and the Office of Management and Budget issued a strategy with goals, actions, and time lines for improving the cybersecurity workforce. In addition, laws such as the Federal Cybersecurity Workforce Assessment Act of 2015 require agencies to identify IT and cyber-related positions of greatest need. Further, other on-going activities have the potential to assist agencies in developing, recruiting, and retaining an effective cybersecurity workforce. For example:

- *Promoting cyber and science, technology, engineering and mathematics (STEM) education*.—A center funded by DHS developed a kindergarten to 12th grade-level cyber-based curriculum that provides opportunities for students to become aware of cyber issues, engage in cyber education, and enter cyber career fields.
- *Cybersecurity scholarships*.—Programs such as Scholarship for Service provide tuition assistance to undergraduate and graduate students studying cybersecurity in exchange for a commitment to Federal service.

[6] FedRAMP is a Government-wide program intended to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud computing products and services.

[7] The Trusted Internet Connection program is intended to improve security by reducing and consolidating agency external network connections and by providing centralized monitoring at a select group of access providers.

- *National Initiative for Cybersecurity Careers and Studies*.—DHS, in partnership with several other agencies, launched the National Initiative for Cybersecurity Careers and Studies in 2013 as an on-line resource to connect Government employees, students, educators, and industry with cybersecurity training providers across the Nation.

If effectively implemented, these initiatives, laws, and activities could further agencies' efforts to establish the cybersecurity workforce needed to secure and protect Federal IT systems.

Question 3. What specific challenges does DHS face in protecting or assisting the protection of .gov assets that are owned by other agencies?

Answer. One of the challenges DHS may face in protecting or assisting the protection of .gov assets that are owned by other agencies is having limited insight into what .gov assets the agencies actually own. Agencies may not have complete inventories of the hardware, software, and firmware on their networks. Additionally, if the agencies do have such inventories, they may be reluctant to share them with DHS.

Another challenge is that DHS may lack visibility into the architecture and structure of the agencies' computing environments, networks, and interconnections with other networks. Agencies may not be willing to allow DHS access to scan and monitor their internal networks thereby limiting DHS's capability to have first-hand knowledge of the security configurations of the networks.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR CHRIS JAIKARAN

Question 1. At the hearing we discussed DHS's NCPS and CDM programs. What other actions can DHS take to assist Federal agencies with protecting their information and information systems?

The National Cybersecurity Protection System (NCPS) monitors and analyzes traffic between the public internet and agency networks. With certain tools, NCPS may also block malicious internet traffic. The Continuous Diagnostics and Mitigation (CDM) program scans agency networks to discover what is operating on those networks and information about those devices. The results of those scans are combined with threat intelligence to assist system administrators in prioritizing which updates to apply and on Congressional Research Service which systems to focus. Actions that DHS may take to assist Federal agencies with protecting their information and information systems may be considered under two constructs: What the Department may do under existing law; and those for which the Department would need additional Congressional support to perform (either in resources or authorization).

First, under existing authorities and resources, DHS has options to further assist agencies. DHS was granted authorities under the National Cybersecurity Protection Act of 2014 (Pub. L. 113–282) and the Cybersecurity Act of 2015 (Pub. L. 114–113) to provide technical assistance, incident response, and information-sharing capabilities to both Federal and non-Federal entities. The Federal Information Security Modernization Act (Pub. L. 113–283, otherwise known as FISMA) provided further guidance on the scope and type of technical assistance DHS may provide to Federal entities. Such assistance may include conducting evaluations of agency networks to determine how vulnerable systems are, analyzing data on agency networks, and providing technologies to mitigate threats with or without reimbursement. FISMA further allows DHS to issue binding operational directives (BODs). BODs are memoranda from the Secretary of Homeland Security to other Department and agency heads compelling them to take action to secure information technology systems. DHS may exercise any of these authorities with greater frequency or through novel approaches to further assist agencies. For instance, DHS may opt to issue BODs for a greater number of security purposes. However, depending on the type of activity required by that BOD, DHS may lack a way of independently verifying agency compliance with the required action. Without that verification and subsequent reporting to OMB on compliance future BODs run the risk of being ignored by the agencies. DHS could alternatively opt to prioritize on-site technical assistance to Federal agencies so the agency may use analysts to hunt for and identify security vulnerabilities and develop a custom plan to address those vulnerabilities. However, prioritizing these types of services to Federal agencies could result in fewer of these types of services being available for the private sector, because DHS has a limited

number of teams (the DHS fiscal year budget justification requested additional funds for more teams).[1]

Options exist which would require additional Congressional action for DHS to provide further assistance to agencies. FISMA allows for DHS to provide technologies to mitigate threats to agencies with or without reimbursement. To date, DHS provides monitoring of traffic coming in and out of agency networks, but not for system activity inside the external perimeter of an agency network. DHS's CDM program discovers end-points and vulnerabilities on end-points inside that perimeter, but does not look for malicious activity on-going inside the network. Discovering malicious activity inside an agency's network may be an area where DHS can expand its portfolio of protection technologies-borrowing from the NCPS and CDM models to build and procure tools, and manage the deployment and operations of those tools once installed at agencies. Alternatively, DHS could spend additional resources and bolster the programs they currently operate. A criticism of NCPS is that it is a signature-based system; The system relies on having previously seen an indicator of the bad traffic before taking action. DHS is currently conducting a pilot program on non-signature-based solutions for NCPS.[2] Additional resources could be applied to expand this program so that a greater number of agencies may more rapidly take advantage of it.

Question 2. What does DHS need to consider to ensure that CDM objectives and requirements keep pace with the rapidly-evolving nature of cyber threats?

Answer. CDM uses tools that scan agency networks for end-points running on those networks, identify vulnerabilities inherent on those end-points (such as running an outdated version of software), and display those results on a dashboard for system administrators to analyze. The results of the scans are then coupled with threat intelligence to determine which vulnerabilities are under exploit, which provides system administrators with a way to prioritize their greatest risks for remediation. CDM allows system administrators to address the vulnerabilities on their systems, informed by, but agnostic to, what threat actors are doing or motivated by. CDM helps system administrators discover what vulnerabilities are on their system, but does not address concerns of how hackers exploit those vulnerabilities or which systems hackers are likely to target. Because the program is internal-looking, the evolving nature of threats is an indirect concern. CDM is a program that focuses more on ensuring systems are as secure and resilient as they can be, regardless of what threats exist.

While the CDM program as a whole is threat-agnostic, the benefit the dashboard provides to system administrators (both informing them of their vulnerabilities and alerting them to vulnerabilities under exploit by adversaries) is concerned with evolving threats. Ensuring that threat analytics remains a part of the CDM program, and can be displayed in a way to system administrators so that they can easily prioritize limited resources to remediating the greatest risks, is a key element of the program. DHS could seek to bolster relationships with the intelligence community and security researchers so that the National Cybersecurity and Communications Integration Center (NCCIC) maintains situational awareness of evolving threats and how those threats are being implemented. Once the organization has knowledge of those threats, they could then integrate that information into CDM to reach Federal agencies. Additionally, DHS could purchase cyber threat indicators from security companies to include in their in-house threat reporting and to inform the CDM program about which vulnerabilities are of greatest risk.[3]

DHS operates other programs that are more concerned with threats. Understanding threat actors, their motivations, their targets, and their techniques helps DHS produce relevant mitigation strategies to share with agencies and critical infrastructure entities. One potential limitation of CDM arises if the program identifies a vulnerability under active exploit by a threat actor, but the vendor who provided the product has not produced a patch for the vulnerability. In an instance like this, DHS's tools would likely be able to identify the weakness but not provide a recommendation for securing it. Instead, DHS may resource a team to develop other mitigating strategies that agencies may deploy in the interim—so as to provide the

---

[1] Jeh Johnson, "Remarks by Secretary of Homeland Security Jeh C. Johnson on the State of Homeland Security," speech, February 11, 2016, at *https://www.dhs.gov/news/2016/02/11/remarks-secretary-homeland-security-jeh-c-johnson-state-homeland-security.*

[2] Jeanette Manfra, "Regarding Federal Network Cybersecurity," written testimony, March 28, 2017, at *http://docs.house.gov/meetings/HM/HM08/20170328/105778/HHRG-115-HM08-Bio-ManfraJ-20170328.pdf.*

[3] "Cyber threat indicator" is defined in the Cybersecurity Information Sharing Act of 2015, in 6 USC § 1501 (6).

vulnerable agency with positive actions they may undertake to shore up their security.

Question 3. One of the priorities of this committee is to ensure the Federal Government is effectively leveraging innovative cybersecurity technologies. The private sector today is able to readily leverage the latest security services through commercial cloud capabilities. What role should DHS play in helping Federal agencies consider and potentially migrate to the cloud?

Answer. Through the use of cloud-enabling technologies, entities may take advantage of a provider's processing power, storage capacity, or a combination of both to add additional capacity, capability, or flexibility to their own information technology systems. Cloud providers furnish computing services to customers through one of three service models:[4]

1. Infrastructure as a Service.—In this model the cloud provider provides the hardware and network connection for their customer, who in turn installs and maintains the applications on those servers to meet their needs. Products in which customers rent processing power or storage from a provider are examples of Infrastructure as a Service.

2. Platform as a Service.—In this model the cloud provider provides the hardware, connectivity, and underlying appliance onto which customers move their data. Products which provide databases or provide a development environment are examples of platform as a service.

3. Software as a Service.—In this model the cloud provider provides the hardware, connectivity, and software to the customer, along with management of the service. Products in which a customer only needs a user name and password because the entire user interface, application, and back-end are provided on-line are examples of Software as a Service.

Cloud environments can be public (i.e., leasable through the internet), or private (i.e., built and managed in-house or by a partner) and accessible without a connection to the public internet, or a combination of the two.[5] There have been previous attempts to assist agencies in shedding their current, in-house system architecture and migrate to cloud providers.[6]

DHS currently plays a role in assisting agencies in their migration to cloud technology through FedRAMP. FedRAMP is a Federal program run out of GSA which examines public cloud providers and assesses their security in order to assist agencies in choosing a cloud provider and using their services. DHS is a member of the FedRAMP Joint Authorization Board (JAB), which provides preliminary authorization for cloud providers to offer services through FedRAMP, and helps in the governance and operations of the FedRAMP program.[7] In addition to being on the JAB, DHS provides expertise and assistance to the GSA in the management of the program.

As agencies consider moving to cloud architecture, they consider their level of risk exposure under their current architecture, their risk exposure by moving to a cloud provider, and weigh the benefits and costs to the migration. DHS may assist agencies in understanding their own risk by performing technical evaluations of their security posture and providing intelligence analysis on threats the agency may face for the mission they perform or the data they store. Possessing this information, agencies may be better-informed in understanding the risks and plotting their future system architecture.

Alternatively, DHS may coordinate agency activities to migrate to cloud infrastructure. Under current authorities, DHS may coordinate information security operations across Government agencies to ensure effective implementation.[8] DHS may compile a series of case studies and recommendations based on agency migrations to cloud providers to assist other agencies in evaluating their potential migration to the cloud.

○

---

[4] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800–145, September 2011, at *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*.

[5] Ibid.

[6] Vivek Kundra, "Federal Cloud Computer Strategy," strategy, February 8, 2011, at *https://www.dhs.gov/sites/default/files/publications/digital-strategy/Federal-cloud-computing-strategy.pdf*.

[7] *www.fedramp.gov*.

[8] 44 U.S.C. § 3553 (b).