CDM: GOVERNMENT PERSPECTIVES ON SECURITY AND MODERNIZATION

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

AND THE

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MARCH 20, 2018

Serial Nos. 115–55 and 115–69

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov and http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

30–791 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
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
RON ESTES, Kansas
DON BACON, Nebraska
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*
STEVEN S. GIAIER, *Deputy Chief 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
BRIAN K. FITZPATRICK, Pennsylvania
DON BACON, Nebraska
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)*

KRISTEN M. DUNCAN, *Subcommittee Staff Director*

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

TREY GOWDY, South Carolina, *Chairman*

JOHN J. DUNCAN, JR., Tennessee
DARRELL E. ISSA, California
JIM JORDAN, Ohio
MARK SANFORD, South Carolina
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
BLAKE FARENTHOLD, Texas
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
DENNIS A. ROSS, Florida
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama
JAMES COMER, Kentucky
PAUL MITCHELL, Michigan
GREG GIANFORTE, Montana

ELIJAH E. CUMMINGS, MARYLAND, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
BONNIE WATSON COLEMAN, New Jersey
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
JIMMY GOMEZ, Maryland
PETER WELCH, Vermont
MATT CARTWRIGHT, Pennsylvania
MARK DESAULNIER, California
STACEY E. PLASKETT, Virgin Islands
JOHN P. SARBANNES, Maryland

SHERIA CLARKE, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
TROY STOCK, *Subcommittee Staff Director*
MEGHAN GREEN, *Counsel*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

PAUL MITCHELL, Michigan, *Vice Chair*
DARRELL E. ISSA, California
JUSTIN AMASH, Michigan
BLAKE FARENTHOLD, Texas
STEVE RUSSELL, Oklahoma
GREG GIANFORTE, Montana

ROBIN L. KELLY, Illinois, *Ranking Minority Member*
JAMIE RASKIN, Maryland
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois

CONTENTS

CDM: GOVERNMENT PERSPECTIVES ON SECURITY AND MODERNIZATION

Tuesday, March 20, 2018

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION, JOINT WITH THE
COMMITTEE ON OVERSIGHT AND
GOVERNMENT REFORM,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
WASHINGTON, DC.

The subcommittee met, pursuant to notice, at 2:38 p.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe (Chairman of the subcommittee) presiding.

Present: Representatives Ratcliffe, Hurd, Katko, Donovan, Fitzpatrick, Bacon, Jackson Lee, Langevin, Lynch, Demings, Connolly, and Krishnamoorthi.

Mr. RATCLIFFE. The Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection and the Committee on Oversight and Government Reform Subcommittee on Information Technology will come to order. The subcommittees are jointly meeting today to receive testimony regarding the Department of Homeland Security's continuous diagnostics and monitoring program. I now recognize myself for an opening statement.

This is the second hearing this year that the Subcommittee on Cybersecurity and Infrastructure Protection has held on the Continuous Diagnostics and Mitigation, or CDM, Program. That is because I see real value in the goals of CDM, not only for cybersecurity but also for improving the efficiency of the information technology across the board. To that end, I am pleased to be holding this hearing today jointly with my good friend from Texas, Congressman Will Hurd, who will be joining us shortly and who has been a leader on IT modernization issues as the Chairman of the Subcommittee on Information Technology. I welcome our friends from the Oversight Committee to the CDM conversation today.

I believe that DHS's CDM Program has great potential to drive progress on a number of cybersecurity issues, from network visibility to data-centric security and from the role of increased automation of security tasks to the role of artificial intelligence. So the question that I have for this panel today is what can Congress do to make sure CDM capabilities are being rolled out to keep pace with the evolving threat landscape?

The Government has a pretty checkered past when it comes to IT investments and the ability of Federal agencies to provide effec-

tive cybersecurity. While CIOs are the point of accountability on all things IT at their respective agencies, every stakeholder has to recognize their role in supporting CIOs. But this is a hearing about finding solutions and ensuring that the Federal Government is on the right track.

I think every agency represented today has some IT investment or application that did not produce the kind of results the American people, the American public needs and deserves from their taxpayer dollars. That is not to mention the profoundly damaging data breaches that have plagued Federal agencies.

We simply have to get a handle on the cyber threats we are facing. I believe that CDM is part of that solution. This hearing is about learning from the initial roll-out and progress of CDM phase 1, plans to move through phase 2, and, perhaps most importantly, what is and what should be the long-term vision of CDM?

Obviously, part of today's hearing will involve a discussion about the resources necessary to invest in top-of-the-line security technologies, but at its core, cybersecurity is more than an issue of technology; it is an issue of governance, of process, and leadership. We have to get the strategies and vision for CDM right so that our investments don't throw good money after bad. To that end, I intend today's hearing to include a robust conversation about the metrics necessary to measure not only the implementation of CDM but also the effectiveness of the program as well. CDM is about maintaining more secure systems and a better understanding of the risk posture of the Federal enterprise, but it also represents a continuing mission and establishes the kind of structure necessary for us to evolve.

To that end, I welcome your thoughts, not only about the CDM capabilities but also about the ultimate goal of providing network and system defenders with the data and tools necessary to do their jobs well and at the pace to combat the threats that they face. What is CDM's value-add to the people on the lines of this conversation? It is the Federal agencies' CIOs that are ultimately accountable for bad investments or data breaches. So this is really about getting you the authorities, tools, and resources that you need to get the job done.

As we continue this conversation, I look forward to hearing from stakeholders, as we did at last month's hearing, as we will continue to make sure that we are getting CDM right. CDM is an ambitious program that I believe has the framework of providing the kind of cybersecurity that the American people deserve from a Government that they entrust with their most valuable personal and, in some cases, irreplaceable information.

I want to thank the witnesses for their time, and I look forward to your testimony today.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

MARCH 20, 2018

This is the second hearing this year that the Subcommittee on Cybersecurity and Infrastructure Protection has held on the Continuous Diagnostics and Mitigation or CDM program. That is because I see real value in the goals of CDM not only for

cybersecurity, but also for improving the efficiency of information technology across the board.

To that end I am pleased to be holding this hearing today jointly with my good friend from Texas, Mr. Hurd—who has been a leader on IT modernization issues as the Chairman of the Subcommittee on Information Technology.

We welcome our friends from the Oversight Committee to the CDM conversation.

I believe that DHS's CDM program has great potential to drive progress on a number of cybersecurity issues—from network visibility to data-centric security and from the role of increased automation of security tasks to the role of artificial intelligence.

So the question I have to this panel today is—what can we as Congress do to make sure CDM capabilities are being rolled out to keep pace with the evolving threat landscape?

The Government has a checkered past when it comes to IT investments and the ability of Federal agencies to provide effective cybersecurity. And while CIO's are the point of accountability on all things IT at their respective agencies, every stakeholder has to recognize their role in supporting CIOs.

But this is a hearing about finding solutions and ensuring the Federal Government is on the right track.

I think every agency represented today has some IT investment or application that did not produce the kinds of results the American public needs and deserves for their taxpayer dollars. And that is not to mention the profoundly damaging data breaches that have plagued Federal agencies.

We have to get a handle on the cyber threats we are facing and I believe CDM is part of the solution.

This hearing is about learning from the initial rollout and progress of CDM phase 1, plans to move through phase 2, and perhaps most importantly what is and should be the long-term vision of CDM.

Obviously, part of today's hearing will involve a discussion about the resources necessary to invest in top-of-the-line security technologies.

But at its core cybersecurity is more than an issue of technology, it is an issue of governance, process, and leadership. We have to get the strategies and vision of CDM right, so that our investments don't throw good money after bad.

To that end, I intend today's hearing to include a robust conversation about the metrics necessary to measure not only the implementation of CDM but the effectiveness of the program as well.

CDM is about maintaining more secure systems and a better understanding of the risk posture of the Federal enterprise. But it also represents a continuing mission and establishes the kind of structure necessary to evolve.

To that end I welcome your thoughts not only about the CDM capabilities, but also about the ultimate goal of providing network and system defenders with the data and tools necessary to do their jobs well and at the pace to combat the threats they face.

What is CDM's value-add to the people on the lines of this conversation?

It is the Federal agency CIO's that are ultimately accountable for bad investments or data breaches, so this is really about getting you the authorities, tools, and resources you need to get the job done.

As we continue this conversation I look forward to hearing from stakeholders as we did at last month's hearing, and what we will continue to do to make sure we are getting CDM right.

CDM is an ambitious program that I believe has the framework of providing the kind of cybersecurity the American people deserve from a Government they entrust with their most valuable, personal, and in some cases, irreplaceable information.

I want to thank the witnesses for their time and I look forward to their testimony.

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

We are pleased to have a distinguished panel of witnesses before us today on this very important topic. Mr. Max Everett is the chief information officer for the Department of Energy. Mr. Everett held a variety of information technology leadership positions in Government and the private sector before joining DOE in June 2017.

We certainly look forward to your perspectives today, sir.

Mr. Scott Blackburn is the executive in charge of the VA's Office of Information and Technology and has served in that capacity

since October 2017. Prior to joining the VA, Mr. Blackburn served in the Army until 2003.

Thank you for that service as well, sir, and thanks for being here.

Mr. David Garcia is the chief information officer for the Office of Personnel Management. Mr. Garcia previously served as the chief information officer for the State of Maryland.

Sir, thank you to being here with us today.

Finally, Mr. Kevin Cox is the program manager for CDM in the National Protection and Programs Directorate at the Department of Homeland Security. Before joining DHS, Mr. Cox was the deputy chief information security officer at the Department of Justice. We look forward to gaining your insights on your interagency experiences.

Mr. CONNOLLY. Mr. Chairman.

Mr. RATCLIFFE. Yes, sir.

Mr. CONNOLLY. I serve as the Vice Ranking Member of the Oversight and Government Reform Committee. In the absence of Mr. Cummings, I do have an opening statement I would like to read.

Mr. RATCLIFFE. I recognize the gentleman for his opening statement.

Mr. CONNOLLY. I thank the Chairman for his courtesy. I want to thank you and Chairman Hurd for holding today's hearing to examine the status of the Department of Homeland Security's Continuous Diagnostics and Mitigation Program.

Initiated in 2013 by the Department of Homeland Security, the CDM Program provides other Federal agencies hardware, software, and services through contracting vehicles to strengthen the security of Federal networks. As you indicated, Mr. Chairman, desperately needed.

CDM has great potential to help agencies secure networks by providing data to agencies on their attack surface, who has access to their networks, and how users access those networks. This will eventually allow agencies to monitor their traffic and network activities and identify areas of concern.

Just this week, we were reminded, albeit in the private sector, of additional Russian attacks on our grid. So we know the attack—or the threat is real. However, the lack of adequate funding for CDM has impeded full deployment of the program. The President's budget for fiscal year 2019 requested $237 million for the CDM Program as part of an $815 million request for cybersecurity funding at DHS.

As in previous years, the $237 million is not just for DHS to oversee the procurement and operations associated with CDM but also for individual agencies to implement activities related to the program, and so it gets disbursed pretty quickly.

When funding from DHS does not completely cover the costs to agencies implementing CDM, agencies are left to find funding among other information technology priorities. However, at a time when so much of Federal IT spending is simply to operate and maintain legacy systems, it will continue to be a challenge for agencies to find the money for net new investment in CDM, which is certainly something we support on a bipartisan basis.

The MGT Act we just passed into law, and I was proud to be an original Democratic co-sponsor, may help agencies with funding challenges by allowing agencies to establish working capital funds to reinvest IT savings in the enterprise and to transition to cloud computing and other innovative technologies and to enhance cybersecurity. The MGT Act also authorized the centralized technology modernization fund at $250 million for each of fiscal years 2018 and 2019, for a total of $500 million. Once the TMF is funded, agencies can borrow from that fund to finance large IT modernization projects and enhance the CDM process.

I was happy to join with Chairman Hurd in a letter to the Appropriations Subcommittee on Financial Services and General Government Subcommittee last week to support appropriating the total $250 million for TMF for fiscal year 2019. Congress and this administration must recognize that, unless there is a significant amount of money agencies can use to upgrade old IT systems that are critical for their mission and that can be encrypted—that is to say new investments that can be encrypted—agencies will not only be able to address the low-hanging fruit and will not be incentivized to take on the larger projects that are complicated, take a long time, and could be prone to cyber attack.

The shortage of qualified Federal employees to work on IT and cybersecurity has also hindered DHS and agency efforts to implement CDM. While agencies are working to attract the talented individuals they need to upgrade their IT systems and to defend against malicious cyber intrusions, the administration and some in Congress are taking actions that I think will make it more difficult to recruit and retain the skilled work force of the future. Disparagement of the work force, freezing salaries, extending probationary periods for new hires from 1 to 2 years—these are not helpful, especially if we are targeting the millennial generation that expects so much more in the workplace. So I would hope we keep that in mind too, because that is part and parcel of what we are talking about here.

So I certainly welcome this hearing. I think we have put some legislative tools in place that we think can create a structure that will foster CBM at DSH and elsewhere. We certainly look forward to hearing the testimony today about how we can do that better.

Thank you, Mr. Chairman.

[The statement of Ranking Member Connolly follows:]

STATEMENT OF RANKING MEMBER GERALD E. CONNOLLY

MARCH 20, 2018

Thank you Chairman Hurd and Chairman Ratcliffe for holding today's hearing to examine the status of the Department of Homeland Security's Continuous Diagnostics Mitigation (CDM) program. Initiated in 2013 by the Department of Homeland Security (DHS), the CDM program provides other Federal agencies hardware, software, and services through contracting vehicles to strengthen the security of Federal networks.

CDM has great potential to help agencies secure their networks by providing data to agencies on their attack surface, who has access to their networks, and how users access those networks. This will eventually allow agencies to monitor their traffic and network activities and identify areas of concern.

However, the lack of adequate funding for CDM has impeded full deployment of the program. The President's budget for fiscal year 2019, requested $237 million for the CDM program as part of an $815 million request for cybersecurity funding at

DHS. As in previous years, the $237 million is not just for DHS to oversee the procurement and operations associated with CDM, but also for individual agencies to implement activities related to the program. When funding from DHS does not completely cover the cost to agencies of implementing CDM, agencies are left to find funding among other information technology (IT) priorities. However, at a time when nearly 80 percent of Federal IT spending is on operations and maintenance of legacy IT systems, it will continue to be difficult for agencies to find money for CDM among other IT projects.

The MGT Act may help agencies with funding challenges by allowing agencies to establish working capital funds to reinvest IT savings to retire legacy IT systems, transition to cloud computing or other innovative technologies, and enhance cybersecurity. The MGT Act also authorized a centralized Technology Modernization Fund (TMF) at $250 million for each of fiscal years 2018 and 2019, for a total of $500 million. Once the TMF is funded, agencies can borrow from the fund to finance large IT modernization projects. I was happy to join Chairman Hurd on a letter to the House Appropriations Subcommittee on Financial Services and General Government Subcommittee last week in support of appropriating the total $250 million to the TMF for fiscal year 2019. Congress and this administration must recognize that unless there is a significant amount of money agencies can use to upgrade old IT systems that are critical to their mission, agencies will only be able to address the "low hanging fruit" and will not be incentivized to take on the larger projects that are complicated and prone to a cyber attack.

The shortage of qualified Federal employees to work in IT and cybersecurity areas has also hindered DHS and agency efforts to implement CDM. While agencies are working to attract the talented individuals they need to help upgrade their IT systems and defend against malicious cyber intrusions, the administration and the Majority in Congress are taking actions that make it difficult for Federal agencies to compete with the private sector in recruiting and retaining skilled cybersecurity and IT professionals. In the administration's budget proposal for fiscal year 2019, the President is seeking a pay freeze for all civilian Federal employees. The administration also proposed reducing retirement benefits for current and future Federal employees, changing how the Government contribution to health plans are calculated, and amending how paid leave is determined. Last year, the House of Representatives passed legislation to increase the probationary period for Federal employees from 1 year to 2 years.

It is no wonder why agencies not only have trouble recruiting the IT and cyber workforce they need, but why they are also losing employees to the private sector. Many seeking to enter public service understand that the Government cannot pay as much as the private sector, but reducing retirement benefits, instituting a short-sighted pay freeze, and increasing trial periods for a highly sought-after workforce is counterproductive and only makes it harder to implement the "sweeping transformation of the Federal Government's technology" promised by the President.

Mr. RATCLIFFE. I thank the gentleman.

Again, I remind other Members of the committee that they may submit opening statements for the record as well.

[The statements of Ranking Members Thompson and Richmond and Honorable Jackson Lee follow:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 20, 2018

The Continuous Diagnostics and Mitigation (CDM) program is a key part of our National approach to secure Federal networks, which Americans rely on to store some of our most sensitive National data—from health records and Social Security Numbers to the holdings of critical infrastructure owners and operators and National security documents.

Over the past decade, we have seen the number of cyber attacks against Federal agencies rise exponentially. According to the Government Accountability Office cyber attacks have risen by more than 1,000 percent since 2006.

The Office of Management and Budget reports that Federal agencies endured more than 35,000 cybersecurity incidents last year alone.

Some of the officials testifying on today's panel know all too well how much damage can flow from a high-profile breach.

For instance, the Veterans' Affairs Department reported in 2013 that its databases had been hacked by no less than eight foreign governments.

And in 2015, the Chinese government infiltrated the Office of Personnel Management's systems and accessed the personal information of more than 22 million past and present Federal employees.

Last week, we turned our attention to bold attacks carried out by the Russian government in 2016 to access and gain control of the central command centers that support our electrical grid, nuclear power plants, and our water supply.

Even the Secretary of Energy admitted that he was "not confident" in the ability of the Federal Government to counter foreign adversaries in cyber space.

These hackers show no signs of slowing down. Instead, they have only grown more aggressive and more sophisticated.

Federal agencies need robust cybersecurity now more than ever—and CDM has the potential to be an important line of defense.

Through the CDM program, DHS works with Federal agencies to procure cybersecurity tools and services to fend off cyber attacks.

The program works in tandem with EINSTEIN to keep out unauthorized traffic, continuously monitor for threats, improve visibility of network assets, and prioritize efforts to correct vulnerabilities.

Unfortunately, Federal agencies have been slow to adopt and fully deploy CDM technologies.

In a hearing earlier this year, we learned that agencies and CDM vendors are struggling to compensate for a lack of cyber expertise among agency personnel.

The witnesses told us that these employees need to be better trained on how to use CDM tools in order to reap all the security benefits they provide.

We also heard that, after 5 years, agencies still do not have a full accounting of all the devices connected to their networks.

Agencies need this visibility, since they cannot protect what they do not know they have.

These obstacles are compounded by the staggering number of cyber vacancies throughout the Federal Government, both for rank-and-file civil servants, as well as key leadership positions.

Far too many agencies are still operating without a permanent chief information officer in place.

We need to understand the challenges agencies are facing when it comes to purchasing, installing, and deploying CDM capabilities, and we need to make sure you have the resources, support, and statutory authority necessary to continue moving forward.

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

MARCH 20, 2018

The Continuous Diagnostics and Mitigation (CDM) program is a key component of the Department of Homeland Security's (DHS) overall effort to protect the ".gov" domain. Through CDM, DHS works with agencies to procure cybersecurity tools and services that will enable them to identify and defend against attacks. These tools are increasingly important in today's security environment.

Every year, Federal networks get hit by tens of thousands of attempted intrusions—many of them highly sophisticated, state-sponsored attacks. According to the Office of Management and Budget, Federal agencies endured over 35,000 cybersecurity incidents in fiscal year 2017, which is higher than previous years. As initially envisioned, CDM would provide Federal agencies with the information and tools necessary to protect their networks, including:

- What devices and assets are on an agency's network?
- Who has access to an agency's network, including those parts of the network reserved for privileged users?
- What happens on the network, and how data is stored and protected?

Unfortunately, agencies have been slow to realize the potential benefits of CDM due to unanticipated implementation challenges. For example, Federal agencies struggled to complete the difficult task of identifying all of the devices, assets, and endpoints on agency networks. Moreover, when the Cybersecurity and Infrastructure Protection Subcommittee held a hearing with CDM contractors in January, witnesses observed that many agencies lack personnel with the appropriate training and expertise to reap the full value of CDM tools, particularly the dashboards.

This subcommittee has repeatedly examined cyber workforce challenges throughout the Federal Government, and our witnesses in January reminded us that there is no silver bullet technology can replace human capital. We also learned that, although the CDM program has been in place for 5 years, agencies still do not have

full visibility into the IT assets on their networks. Without this visibility, it is impossible for agencies to know who has access to their networks, and what exactly they need to protect. Today's witnesses can provide an important and informed picture of how CDM tools and services are being adopted and deployed at their respective agencies.

I am interested in knowing not only the status of implementation, but also how these agencies are working with the Department of Homeland Security, and how effectively the Department has been able to respond to agency needs. I also hope to hear what Congress can do to make sure CDM is an effective tool for raising the bar on cybersecurity throughout the Federal Government.

Last week, the Department of Homeland Security and the FBI issued a technical alert on the Russian government's efforts to use cyber tools to target U.S. Government entities. These cyber attacks were carried out over the course of 2016, and parallel Russia's attacks on our electoral system and democratic institutions. It is clear that the Kremlin will continue to be relentless in its assault on our Federal networks, and the networks that support our Nation's critical infrastructure. And, we know that China, Iran, and North Korea are sophisticated cyber actors that are constantly working to build a more robust cyber "arsenal" that could be used against our Federal networks. We must remain vigilant in protecting the .gov, and do everything in our power to ensure the Federal Government has the resources needed to act quickly to protect itself.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

MARCH 20, 2018

Chairman John Ratcliffe and Ranking Member Cedric Richmond, of the House Homeland Committee's Subcommittee on Cybersecurity and Infrastructure Protection; and Chairman William Hurd and Ranking Member Robin Kelly of the House Government Reform's Subcommittee on Information Technology thank you for today's joint hearing on "CDM: Government Perspectives on Security and Modernization."

On January 17, 2018, the Homeland Security Committee's Subcommittee on Cybersecurity and Infrastructure Protection held a hearing on "CDM: the Future of Federal Cybersecurity."

That hearing engaged non-Government stakeholders who provided Members of the subcommittee on Homeland Security with the opportunity to learn more about the Continuous Diagnostics and Mitigation (CDM) program, a key component of the Department of Homeland Security's (DHS) overall effort to protect Federal network.

Today's hearing will give Members an opportunity to hear agency perspectives on the Continuous Diagnostics and Mitigation (CDM) program.

Our witnesses will provide valuable insight into the civilian agency experience with the rollout of CDM throughout the Federal Government:

WITNESSES

- David Garcia, Chief Information Officer, Office of Personnel Management;
- Max Everett, Chief Information Officer, Department of Energy;
- Scott Blackburn, Executive in Charge, Office of Information Technology, Department of Veterans Affairs; and
- Kevin Cox, Program Manager, Continuous Diagnostics and Mitigation, Office of Cybersecurity & Communications, Department of Homeland Security (Democratic Witness).

The Continuous Diagnostics and Mitigation program is an active approach to fortifying the cybersecurity of Government networks and systems.

The security of Federal agency networks has been a major concern of mine since I chaired the Subcommittee on Transportation Security, which at that time had jurisdiction over cybersecurity issues.

Earlier this year, the House passed H.R. 3202, the Cyber Vulnerabilities Disclosure Act, which I introduced to address the need for effective and aggressive action to deal with the threat of Zero Day Events.

H.R. 3202 requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

I have also introduced last Congress and again this Congress a bill to address the cybersecurity workforce shortage in the Federal Government.

The bill H.R. 1981, Cyber Security Education and Federal Workforce Enhancement Act, which will establish the process for looking outside of DHS and within its ranks to solve the shortage of cybersecurity professionals.

The solution is making sure that from early childhood education through University programs young people are prepared with the fundamentals needed to excel in course work associated with computing security degrees or certification.

The need for a strong cybersecurity posture for our Nation's Federal civilian agency computing networks is essential to a healthy National security posture.

This month, the Office of Management and Budget (OMB) reported that "[Federal] agencies endured 35,277 cybersecurity incidents in fiscal year 2017, a 14 percent increase over 30,899 incidents that agencies reported in fiscal year 2016, with five of the fiscal year 2017 incidents reaching the threshold of 'major incident' due to their impact."

The Continuous Diagnostics and Mitigation or CDM provides Federal departments and agencies with the tools needed to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

The Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources.

It is true that each Federal agency is responsible for protecting its own information systems; however, some agencies, including DHS, play a larger role in Federal network security.

Under the Federal Information Security Modernization Act, DHS is required to deploy technologies to continuously diagnose or mitigate cyber threats and vulnerabilities and make such capabilities available to agencies upon request.

The law essentially codified the CDM program, which DHS is implementing.

DHS entered into partnership with GSA in 2013 to meet the statutory obligation of the Federal Information Security Modernization Act, which facilitated agencies purchase of consistent, compliant technologies that offered "Information Security Continuous Monitoring Mitigation" (ISCM).

The first contract was awarded on August 12, 2013, to 17 companies, supported by 20 subcontractors, that received awards under a $6 billion, 5-year companion Continuous-Monitoring-as-a-Service to deliver diagnostic sensors, tools, and dashboards to agencies.

CDM is an essential part of the Department of Homeland Security's overall effort to protect the civilian Federal network.

Implementation of CDM is being phased in under the process established by DHS using several contractors and subcontractors.

There have been a number of challenges to the process of implementing a Federal-wide CDM program.

DHS encountered a number of unexpected challenges during the rollout of Phase 1.

For example, neither DHS nor the customer agencies anticipated how difficult it would be to identify all the hardware and software assets associated to a network and grossly underestimated the number of agency-connected devices, which delayed the purchase and installation of the necessary sensors.

In May 2016, GAO reported that most of the 18 agencies covered by the CFO Act that had high-impact systems were in the early stages of CDM implementation, and many were proceeding with plans to develop their own continuous monitoring strategies, independent of CDM.

Further, only 2 of the 17 agencies reported that they had completed installation of agency and bureau or component-level dashboards and monitored attributes of authorized users operating in their agency's computing environment.

Due to these unexpected challenges the early estimates of completing Phase 3 by 2017 were not met.

These issues as well as the urgency of protecting Federal agency networks makes it imperative that we have DHS before the committee to provide an update on the CDM program.

I look forward to hearing the testimony from today's witnesses.

Mr. Chairman, I yield back.

Mr. RATCLIFFE. Having already introduced our distinguished panel, I now ask the panel to stand. Raise your right hand so I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. Let the record reflect that the witnesses have answered in the affirmative. You all may be seated.

The witnesses' full written statements will appear in the record.

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

STATEMENT OF MAX EVERETT, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY

Mr. EVERETT. Good afternoon, Chairman Hurd, Chairman Ratcliffe, Ranking Member Connolly, Ranking Member Richmond, and the rest of the distinguished panel. On behalf of Secretary Perry and Deputy Secretary Brouillette, I appreciate the opportunity to come and talk to you today about CDM and modernization and our implementation at the Department of Energy.

Chairman Hurd, we talked last November at a hearing, and you asked me a very pointed question: Do I know everything that is on all of our viewing networks? My blunt answer had to be no. While that is still the case, I am happy to be here to talk a little more about some of the work and efforts we are making so I can change that no into a yes.

First, as the Department CIO, I report directly to the Secretary and deputy secretary, which I think is a critical, critical thing for all CIOs in government. I think it is also important because our Secretary and deputy secretary have made cybersecurity a priority, not only for our internal networks but also in our role as a sector-specific agency to the energy sector, and I think that is critical. Our Secretary and deputy secretary understand very well the importance of knowing everything that is on our network as a first step to having basic cybersecurity.

The Secretary and deputy secretary fully support our enterprise plan of action and have directed me to move with all due haste in rolling out CDM capabilities across our networks where we have many gaps, including at our National labs, our sites, and at the Power Marketing Administrations. In both the public sector and private sector, one of our challenges is, frankly, we are moving to a new model. The old model was staff augmentation. The old model was counting contractors. We are moving to a new model, and that new model is around managed services and automation. That is a significant challenge because most of us in Government and, frankly, even many in the beltway vendor community have not really caught up yet. That is an on-going challenge for us. I know it very well as a former Federal contractor.

In the Federal work force, I need people not only with the technical skills to use all these new tools, but I also need people who have customer service ability. I need people who can understand organizational management, people that understand business process. We've got to find, as you spoke about Congressman Connolly, we've got to have a new model to bring in the talent that we need to achieve the goals that we're talking about.

I believe that CDM and modernization go hand-in-hand. Chairman, as you talked about earlier, CDM actually can be a great driver for modernization, the information and the data we get from that can help us in prioritizing what we modernize and putting those priorities out front. In turn, I believe modernization sets out the platforms that will allow us to do the automation that makes CDM more and more valuable as we go along.

It is essential for the incentives for both the CDM Federal contracts folks, as well as the vendors, to be aligned to the right goals. I think that's one of our other critical elements here, is to make sure that we have incentivized folks to go for our goals. Our goals are not how many tools we have placed in the environment or necessarily the time lines; our goals are to provision and provide secure and efficient capabilities to meet our missions. So we've got to find some ways to make sure that our incentives match that goal.

I do want to mention, while we are here, I want to thank Kevin Cox, one of my fellow panelists, as well as and Mark Kneidinger at DHS. I've had multiple opportunities to interact with them and their teams. My team meets regularly with them. I want to give them kudos because, very frankly, this program been around for a few years, and really and especially in the last year, they've done significant work in making the program more collaborative. I think we need to continue that process of collaboration. One of the challenges, to be very frank with you, about CDM is that many departments have perceived this as a program being done at them rather than with them. I think Kevin and Mark Kneidinger and their team have done a lot to reverse that viewpoint.

I want to mention that, again, visibility that CDM brings is only the first step. It's going to require action. We need to focus on making sure that the things we get out of CDM at the Federal level and the Departmental level are actionable information that we can move forward with. We've got to do that, and we know that you're going to hold us accountable for doing that.

I want to give you a quick example: One my labs used a CDM-like capability last year to help them find some unmanaged cloud services in their environment and the steps they took around customer service admission resulted in provisioning new, better, and more secure capabilities and removing those things which were a management risk out of the environment. We want to find more opportunities to do exactly that kind of thing across the Department and across the Federal enterprise.

Finally, I do want to mention the MGT Act. The tools—the technology management fund as well as the working capital fund—are critical tools for all of us in the CIO community. I'm happy to report that I've had a lot of progress talking to our CFO shop, and we put in five proposals to OMB for using the technology management fund and are very hopeful that that will be fully funded very soon by Congress.

I want to thank you again for the opportunity to come and talk about this. It is an important issue, and it is a critical tool for us across Government and look forward to answering your questions.

[The prepared statement of Mr. Everett follows:]

PREPARED STATEMENT OF MAX EVERETT

MARCH 20, 2018

Good afternoon Chairmen Hurd and Ratcliffe, Ranking Members Connolly and Richmond, and distinguished Members of the committees. On behalf of the Secretary and deputy secretary of Energy, I thank you for inviting me to testify about the Department of Energy's (DOE or Department) experience with Continuous Diagnostics and Mitigation (CDM) capabilities and tools.

DOE PRIORITIES

As the Department's chief information officer (CIO), I report directly to the Secretary and deputy secretary, properly positioning me to ensure that decision-making processes across the Department factor in Information Technology (IT) and cybersecurity considerations from the outset. The Secretary and deputy secretary have repeatedly emphasized to senior Departmental leadership the importance of weaving cybersecurity into the fabric of DOE policy and operations. They understand that the first step toward protecting information and systems is to have visibility into what is connected to and runs on DOE networks.

Chairman Hurd, at the Federal Information Technology Acquisition Reform Act (FITARA) 5.0 hearing this past November, you asked me whether I could say that I knew everything that was connected to DOE networks. My response then was blunt: I said I could not. Today, 4 months later, while that message has not changed, I am pleased to talk about the work we are doing to be able to answer that question with an emphatic "yes." The lack of fidelity and visibility about what is connected to DOE's networks raises our cybersecurity risk profile to an unacceptable level; urgent action is needed.

The Secretary and deputy secretary are aware of this issue and fully support our enterprise-wide plan of action to obtain fidelity and visibility, enabling DOE to properly protect its networks. We know that CDM tools and capabilities are essential to providing visibility into the content and connectivity of our networks. That is why the Secretary and deputy secretary have given me clear direction to implement CDM as swiftly as possible where gaps exist across the DOE enterprise, including at the National Nuclear Security Administration (NNSA) and its National Laboratories, the Office of Science National Laboratories, the Power Marketing Administrations, plants, and sites. We also recognize that CDM capabilities and automated data collection and flow will enhance DOE's Integrated Joint Cybersecurity Coordination Center (iJC3)—which provides cybersecurity threat analysis, tracks advanced persistent threats, and distributes automated threat information—by providing additional visibility into the network enterprise-wide. Furthermore, CDM will accelerate the availability of the more detailed, relevant, and reliable data necessary to better inform our Enterprise Risk Management processes.

Implementation of CDM Phase 1 and 2 has been accomplished for DOE Headquarters. This is approximately 8 percent of the Department's networked endpoints. I am pleased to report that the Department is looking forward to deploying the common elements of the CDM platform across the DOE enterprise to fill gaps in current capabilities. The Department developed a 180-day strategy to identify and address gaps in CDM Phase 1 and 2 capabilities and to plan implemention of Phase 3 capabilities. This, in combination with mutually reinforcing, on-going IT modernization efforts, will be calibrated to ensure DOE's continued mission success throughout the enterprise.

CDM STATUS

The Department recognizes that sound and comprehensive vulnerability detection requires a multi-dimensional approach involving asset management, automated tools, monitoring of communication channels, and human analysis. We believe that implementing CDM capabilities will play a key role in this multidimensional effort.

Unfortunately, we are still in "catch-up" mode with implementation of CDM enterprise-wide. The Department took a scaled approach to CDM Phases 1 and 2. Before embarking on the larger-scale deployment of CDM across the DOE enterprise, DOE first piloted tools and sensors on the Energy Information Technology Services (EITS) network, which is the network the Office of the CIO directly manages.

We fully implemented CDM Phase 1 tools and sensors across EITS, and successfully tested data transfers with the Department of Homeland Security (DHS). Further, we procured the tools to implement CDM Phase 2 for EITS and are working with a vendor on that implementation. We estimate completion in November 2018.

CDM NEXT STEPS

While we are taking measured, prioritized actions to meet our goals, we appreciate the cooperation and collaboration of our DHS partners. In partnership with DHS, we will conduct a CDM Phase 3 needs assessment—enterprise-wide—to identify and address gaps for the remainder of the Department, including NNSA and its National Laboratories, the Office of Science National Laboratories, the Power Marketing Administrations, plants, and sites. I am pleased to report that we have a high level of confidence in our gap analysis methodology, cost estimates, and due diligence.

In the coming weeks, we intend to utilize the CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) Request for Service (RFS) Process to address Phase 1 and 2 gaps in deployment in addition to Phase 3 and 4 Planning and Implementation requirements. We have incorporated lessons learned from our EITS pilot to streamline the Department's approach and planning as we progress through CDM Phases 3 & 4 with DHS.

My assessment is that CDM capabilities will complement and enhance DOE's IT modernization efforts by helping us identify and prioritize legacy systems in need of remediation. OCIO recognizes that it is not prudent to apply CDM to failing network infrastructures or outdated systems that use legacy software, some of which are no longer supported. While this change will be uncomfortable at first, streamlined and prioritized IT modernization efforts that are fully informed by CDM will, in turn, lay a foundation for further security upgrades, including the components of CDM Phases 3 and 4, and should result in better network security and cost savings through operating efficiencies.

OPPORTUNITIES FOR IMPROVING CDM

Opportunities exist for additional streamlining and acceleration of the CDM implementation process. We will make the most progress when we lead with the areas where shared platforms hold the most obvious and direct opportunities for improved visibility, awareness, and on-going mutual benefits between DOE and Federal agencies. On the other hand, where we have exceptions that require special considerations due to unique environments and mission requirements, we are committed to finding ways to account for their presence on the network, as well as identifying opportunities to adapt or upgrade those systems to make them compatible with enterprise-wide CDM.

We encourage DHS to continue to work actively and collaboratively with their counterpart departments and agencies to develop the CDM dashboard and associated metrics, which need to be usable and actionable by providing relevant threat and vulnerability information. I am confident that the CDM dashboard will provide significant value to the Department as CDM is implemented across the enterprise. The value of the CDM dashboard will be the extent to which it allows us visibility into the networks while providing actionable information and intelligence that can drive real-time decisions that result in increased protection for DOE systems and information. Establishing a credible feedback loop that takes into account the customers' requirements across the Federal enterprise is essential.

We also encourage DHS to continue to actively work with DOE and other departments and agencies in the decision-making processes around the maturation of the CDM program, particularly with regard to contracts, metrics, priority data, and parameters. To have a truly shared platform, we need the information to flow in both directions. Collaboration and cooperation are key to mission success Government-wide. Having a genuine shared platform means having a shared responsibility for the information that we feed into the system, as well as for the information we will receive and use for threat analysis and incident response.

WORKFORCE

At DOE, our people are the key to and foundation of our mission success. We are focused on developing our employees' expertise, expanding our talent pool, and working to optimize the integration of automated systems, such as CDM, to find ways for systems to conduct the automated tasks and large-scale processing for which they are best suited.

Further, we must attract and retain a world-class cybersecurity workforce that has the skills necessary to successfully broker and oversee cloud and managed-services solutions, and make key decisions about how best to use new and rapidly-changing information both tactically and strategically.

CDM AND DIGITAL TRANSFORMATION

In addition to implementing CDM, DOE is conducting a range of IT modernization efforts that are mutually reinforcing with CDM's enhancements to network security. As we continue to implement CDM, it will generate data and visibility that will accelerate these modernization efforts, and the modernization projects will, in turn, provide a robust infrastructure for the deployment of additional tools and capabilities, including CDM.

DOE is currently developing a Digital Transformation Strategy (Strategy), which will provide an enterprise plan of action and include a mechanism to measure results through enterprise requirements for the Department. In addition, we are developing an Enterprise Architecture and Roadmap tied to our Strategy.

Our Strategy will be built on a "Cloud First" policy to transition from service owner to service broker. Consistent with the President's direction in the IT Modernization Report, the Cloud First policy fosters innovation, reduces costs, improves interoperability, scales capacity to match demand, lowers operational costs, and establishes the bedrock for future enterprise capabilities.

We have initiated seven Digital Transformation Work Streams to define enterprise requirements and develop further recommendations for modernization. These are: Trusted Internet Connection, Collaboration Tools and Services, Directory Services, Data Center Optimization, Email, Network Transport, and Mobility.

The Department's Data Center Optimization Work Stream is expected to identify multiple opportunities for IT Modernization from consolidation, virtualization, and cloud migration. Our goal is to move IT workloads to the cloud, maximize virtualization, meet data center closure targets, and retrofit the remaining data centers for optimal energy efficiency while reducing costs.

We also have efforts under way to modernize DOE Headquarters networks to a level consistent with the capacity, agility, and resiliency of modern enterprise networks. This will establish the base for commercial/managed-service implementations of services with engineered and inherent cybersecurity capabilities, such as Infrastructure-as-a-Service and Platform-as-a-Service in support of the Data Center Optimization Initiative, and Enterprise Software-as-a-Service solutions like cloud email and Desktop-as-a-Service, while providing foundational requirements for enhanced cybersecurity tools, products, and capabilities.

CONCLUSION

Enterprise-wide CDM is a high priority for DOE, because of the range of benefits we expect to see from its full implementation. CDM will assist us with other critical and long-overdue efforts, such as IT Modernization, while also providing us with timely, actionable information to help us secure DOE information and systems.

I appreciate the committees' interest in this important topic, and I look forward to continuing to work with our partners in Congress, as well as our colleagues at DHS and across the Federal Government, to achieve our shared goals. It has been my distinct honor to testify before you today, and I would be pleased to address your questions.

Mr. RATCLIFFE. Thank you.

The Chair now recognizes Mr. Blackburn for 5 minutes.

STATEMENT OF SCOTT BLACKBURN, EXECUTIVE IN CHARGE, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS

Mr. BLACKBURN. Good afternoon, Chairmen Ratcliffe and Hurd, and Congressman Connolly, and Members of the subcommittees. Thank you for the opportunity to discuss the progress VA is making toward its deployment of the Continuous Diagnostics and Mitigation Program as well as our information and modernization—information technology modernization effort. Behind me today are Mr. Dominic Cussatt, chief information security officer, and Mr. Gary Stephens, deputy CISO, who oversees the VA CDM Program.

As a proud Army veteran, VA's sacred mission is personal to me. I am a user of VA services. In January, the Baltimore VA operated on my back. I am currently receiving physical therapy at the Washington VAMC. I received part of my care through the Veterans Choice Program. I'm a graduate of the vocational rehab program. I use VA's on-line scheduling tools. I am one of five siblings who have served in uniform. My father, like Congressman Fitzpatrick, was a career FBI agent.

I left the business world in November 2014 to join VA because I didn't believe VA was delivering on its promise to veterans and I wanted to do something about it. I'm very proud of the progress VA has made in this time. Since December 2015, we have increased

veteran trust by 22 percentage points from 47 percent to 69 percent.

For the past 6 months, I've been honored to lead the on-going transformation in IT. It is an exciting time in VA IT. We are replacing VistA with a modern electronic health record that will achieve interoperability within VA, between VA and DOD, and ultimately with community providers in the private health care system. We have not signed the final deal yet with Cerner Corporation, but we hope to be making an announcement soon.

Two weeks ago, we launched a beta version of our Lighthouse Lab, VA's application programming interface, or API, management platform that lets developers build out some standard set of APIs. Lighthouse, formerly known as digital veteran platform, or DVP, will be the API gateway that connects our disparate systems, allowing information exchange and innovation.

Earlier this month, we announced the VA open-API pledge that 11 major health care systems have signed encouraging health care providers to commit to work together with VA to accelerate the mapping of health data to industry standards. We are expanding telehealth and self-service options to include on-line scheduling to improve the veteran experience. We are supporting priorities efforts in the benefits space to include Appeals Modernization and Forever GI bill. We are pushing aggressively on our buy-first strategy to use commercial off-the-shelf solutions to replace expensive and outdated systems.

Next week, we'll launch our new cloud-based software as a service IT management tool, which will streamline internal processes and provide a better end user experience for our employees, allowing them to focus on serving veterans.

We are continuing our data center consolidation to be compliant with FITARA. In fiscal year 2017, we closed 47 data centers, and fiscal year 2018, we are in the process of closing 68 more. Of course, underpinning all of this is improving our cybersecurity through our Enterprise Cybersecurity Strategy Program to guard against cyber threats moving from reactive posture to a proactive, threat-based computer network defense approach.

With cybersecurity in mind, we are committed to protecting veteran information such as mine and limiting access to only those with proper authority. I am proud of the accomplishments and how we are securing VA's IT infrastructure. As of December 2017, we have secured 92 percent of medical devices with vulnerabilities. We have increased PIV enforcement from unprivileged users from 12 percent in 2016 to 91 percent. We've achieved 100 percent enforcement of two-factor authentication for privileged users. We have reduced our unadjudicated software by 94 percent. We have blocked 7.5 billion malware attempts over the past 2 years, and we monitor more than 45 billion emails daily. Through our Enterprise Cybersecurity Strategy Program, ECSP, we managed cybersecurity risk to protect VA information systems. This includes embarking on a change in mindset of how we manage cyber risk. VA's CDM Program is a piece of that larger VA information security continuous monitoring strategy covering 15 continuous diagnostic capabilities which are distributed across its four phases. We can elaborate further on those phases during the course of the hearing.

As part of the CDM effort, we are also documenting and defining existing network hardware application, security products, and configuration control settings currently deployed across the agency to further understand the activity across the network.

Thank you again for the opportunity to discuss our cybersecurity and IT modernization efforts. Ensuring a safe and secure environment for veteran information and improving their experience is our goal. I look forward to your questions.

[The prepared statement of Mr. Blackburn follows:]

PREPARED STATEMENT OF SCOTT BLACKBURN

MARCH 20, 2018

Good afternoon, Chairmen Ratcliffe and Hurd, Ranking Members Richmond and Kelly, and distinguished Members of the subcommittees. Thank you for providing me with this opportunity to discuss the status and progress that VA's OIT is making toward its deployment of the Federal Government's Continuous Diagnostics and Mitigation (CDM) Program and our Information Technology (IT) modernization effort. I am pleased to be joined today by Mr. Dominic Cussatt, chief information security officer, and Mr. Gary Stevens, (acting) deputy CISO, executive director policy and strategy.

The health, safety, welfare, and prosperity of our Veterans are our highest priorities at VA. As one of five siblings who is either a Veteran or still serving in uniform and are all at least the fourth generation of U.S. military Veterans in our family, I take personal pride every day in fulfilling VA's sacred mission, and believe in making VA the best choice for Veterans. We want all Veterans to choose VA like I have, not because it is their only choice, but because we are the best at what we do.

It is an exciting time to be leading OIT with all of the significant strides we are making in information technology. VA is making progress in its cybersecurity and modernization initiatives as well as with Federal Information Technology Acquisition Reform Act (FITARA) and Federal Information Security Management Act (FISMA) compliance. We have announced our intention and will soon be moving forward to replace our decades-old VistA platform with a modern Electronic Health Record (EHR) that will achieve full intra-VA and VA-Department of Defense (DoD) interoperability. The new EHR will also provide the capability for much improved interoperability with community partners. This will be an important development since over 30 percent of our care is currently done outside the Veterans Health Administration (VHA) system in the community.

VA recently announced the launch of a "beta" version of its Lighthouse Lab, a computer platform offering software developers access to tools for creating mobile and web applications that will help Veterans better manage their care, services, and benefits. Eleven leading health care systems have agreed to sign a VA Open Application Programming Interface (API) pledge to accelerate the mapping of health data to industry standards, including the current and future versions of Fast Healthcare Interoperability Resources (FHIR).

VA is continuing to expand telehealth and self-service options, such as on-line scheduling, to improve the Veterans experience. We are pushing aggressively on our "buy first" strategy using commercial off-the-self solutions to replace expensive and outdated systems. Next week, we will launch a new cloud-based, Software as a Service (SaaS) IT service management tool, which will standardize the delivery of IT services and provide our employees with an efficient and consistent end-user experience.

This is the second time in the past several months OIT leadership has appeared before the House Oversight and Government Reform IT Subcommittee. On December 7, 2017, we discussed the progress VA was making toward its transformation efforts, notably our IT modernization effort; FITARA and FISMA compliance; the Electronic Health Record Modernization (EHRM) initiative; and Enterprise Cybersecurity Strategy (ECSS). My testimony today will cover some of those topics with a specific emphasis on the status and progress of the CDM rollout and our IT modernization efforts.

ENTERPRISE CYBERSECURITY STRATEGY PROGRAM (ECSP)

VA, our core constituents, and our external partners are subject to a wide range of cyber threats. Given the high degree of connectivity, interdependence, and reli-

ance on integrated open platform technology, meeting cybersecurity challenges requires strategic attention and collaboration across the VA ecosystem.

Within OIT, we are committed to protecting Veteran information and VA data, as well as limiting access to only those with the proper authority. This commitment requires us to think agency-wide about security holistically. To achieve this end, VA Office of Information Security (OIS) manages cybersecurity risk through VA's ECSP to enable VA to securely fulfill our mission and protect VA information systems.

As part of the ECSP, VA's Enterprise Cybersecurity Strategy is being refreshed to reinforce VA's strategic goals and objectives that inform cybersecurity behaviors at VA. Our principles include, but are not limited to, protection of VA data and Veteran information, evolving VA's resiliency to better adapt to advanced cyber threats, identification and strengthening mission critical systems and infrastructure, modernizing IT, overseeing a secure operational environment, and the recruitment, development, and retention of a talented cybersecurity workforce.

With the establishment of ECSP, we are embarking on a change in mindset of how to manage cyber risk. Through ECSP, we will make prioritized, defensible decisions related to the implementation of cybersecurity projects (that may be technical or procedure-based), align programmatic activities with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and create an integrated and transparent program across each level of the program, which includes Government-wide statutory requirements, VA policy and implementation guidance, organizational cybersecurity capabilities, mission/business processes, and the information system level.

We have recently focused on the following:

- Plans of Action created in response to the fiscal year 2015 Office of Inspector General FISMA audit, which have been closed as of December 31, 2017.
- Eight Strategic Domains created as a result of VA's 2015 Enterprise Cybersecurity Strategy following the release of the Office of Management and Budget (OMB) Cybersecurity Implementation Plan on October 30, 2015.

VA's ECSP is another step forward in VA's commitment to safeguarding Veteran information and VA data within a complex environment. Our strategy establishes an ambitious, yet carefully crafted approach to cybersecurity and privacy protections that helps VA to execute its mission of providing quality health care, benefits, and services to Veterans, while delivering on our promise to keep Veteran information and VA data safe and secure.

VA INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) AND CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

ISCM at VA

In the fall of 2017, we approved our VA ISCM Strategy and the associated ISCM Integrated Project Team (IPT) Charter. The ISCM Strategy and IPT Charter guides VA's continuous monitoring program moving forward detecting and safeguarding systems and data, patient safety, and assisting Veterans after their military career.

Our ISCM program supports a comprehensive VA organizational risk management program. Aligning ISCM to VA's IT risk management program and, in turn, the enterprise risk management program, will provide cost-effective risk management across the organization. ISCM IPT will pursue the following actions to realize this objective:

- Align ISCM activities with risk management activities to provide VA with comprehensive awareness of the security posture and IT infrastructure, assets, and data.
- Align ISCM activities with the on-going authorization process as it is developed, so information systems security controls are evaluated with data to maintain their on-going authorization status.
- Implement a process to identify and prioritize critical ISCM data to collect and monitor, and allow ISCM data to support security control assessments.
- Validate that the ISCM strategic planning process is adequately documented. The ISCM strategic planning process should be transparent and communicated to ISCM stakeholders.

OIT will integrate the current and upcoming ISCM capabilities to effectively evaluate VA's information system posture across the agency. This is accomplished through developing and deploying an end-to-end architecture. ISCM capabilities are being automated to the extent possible by leveraging the Department of Homeland Security (DHS) CDM program, while recognizing some security controls cannot be monitored by automated means. Integrating CDM capabilities into the overall ISCM capabilities and augmenting as necessary with automated and manual monitoring will give VA the ability to meet Veteran and operational needs. As ISCM evolves,

the frequency of monitoring security controls and collecting measurement data stated in VA policy and procedures will be reviewed and revised.

VA's ISCM strategy outlines processes for updating VA directives, handbooks, and standard operating procedures accordingly to align to the ISCM strategy. VA's strategy will be enacted through updates to VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Handbook 6500.3, *Assessment, Authorization, and Continuous Monitoring of VA Information Systems*, and associated ISCM procedures. These documents provide ISCM policy and procedures, in accordance with the NIST Special Publications (SP) 800–137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. VA Handbook 6500.3 was created to establish requirements and responsibilities for VA to confirm compliance with Assessment and Authorization and continuous monitoring requirements for VA information systems as required by FISMA.

Monitoring tools used for ISCM, CDM, and legacy controls are integrated to achieve data synchronization, elimination of data error, and minimization of human interaction. OIT deploys a variety of tools to maintain situational awareness of VA's security posture. Integrating these monitoring tools across VA is the initial action in automating the monitoring, reporting processes. One of the goals of VA's ISCM strategy is to integrate existing and planned ISCM capabilities in order to form a monitoring solution for VA. This includes integrating existing capabilities such as the VA Cyber Security Operations Center Security Incident and Event Manager and the VA Governance, Risk Management, and Compliance tool into CDM dashboards, as part of Phase 1 of CDM development at VA. Integrating these capabilities and others will inform data analysis and reporting on the effectiveness of VA's ISCM program.

The VA ISCM strategy incorporates a variety of performance measures designed for evaluating the effectiveness of our program. Our program measurement sources include:

- *FISMA ISCM Program Maturity Model*.—Summarizes the status of the ISCM program and its maturity based on a five-level scale.
- *Fiscal Year 2017 Chief Information Officer FISMA Metrics*.—Used to assess Federal cybersecurity programs on the progress of their program implementation.
- *NIST CSF*.—Provides guidance on cybersecurity metrics and measurements.
- *VA Enterprise Security Architecture*.—Informs ISCM measures regarding the maturity of current capabilities.

Looking forward, we are seeking additional stakeholders across OIT to join our ISCM IPT to provide insight into how VA currently tracks and reports ISCM-related data. Our IPT stakeholders will assist in the identification of existing ISCM tools, capabilities, and projects to provide a clear indication of how VA currently monitors its network. Ultimately, a more diverse set of stakeholders across our ISCM IPT will enable various groups across VA to work in concert on future ISCM efforts, while also providing varied inputs in order to confirm we are weighing multiple options when our IPT comes to key decision points.

CDM at VA

CDM is a dynamic effort and the needs of different agencies vary. VA's CDM program is a piece of the larger VA ISCM strategy. The VA CDM program covers 15 continuous diagnostic capabilities, which are distributed across its four phases:

- *Phase 1*.—Identify assets on VA network.
- *Phase 2*.—Identify and monitor users on the network.
- *Phase 3*.—Identify what is happening on the network as well as ways to protect it.
- *Phase 4*.—Identify risks on an on-going basis, prioritize risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

VA would like to provide a more in-depth breakdown of where we are within Phase 1 of our CDM program:

- *Hardware Asset Management (HWAM)*—We are currently implementing HWAM tools and integrating these tools to assist in identifying Internet Protocol addresses across the VA network and is intended to assist in the classification of systems and provide reports to our central dashboards. This work covers approximately 2,500 facilities including hospitals, Benefit Centers, Information Technology Centers, VA Central Office, Data Centers, and others.
- *Software Asset Management (SWAM)*—We are currently implementing our SWAM tool, which is designed to inventory software used in the agency and report the information to our central dashboards. Our team is creating lessons learned from HWAM and analyzing them prior to rolling these tools out.

- *Configuration Settings Management (CSM)*—Our team is currently analyzing existing systems. We are identifying security configuration benchmarks that exist for each IT asset type.
- *Vulnerability Management (VUL)*—We are currently implementing our Dashboards, so we can eventually feed into the DHS Federal Dashboard.

We are also documenting and defining existing network hardware, applications, security products, and configuration control settings currently deployed across the agency in order to further understand the activity across the network. OIT is in the midst of providing visibility into the reporting endpoints and depicting them on a CDM dashboard to assist in vulnerability management.

The central dashboards will provide actionable information from HWAM, SWAM, and other security tools for timely remediation of known vulnerabilities as well as transmit data to a DHS Federal dashboard.

OIT documents and provides DHS and OMB its decision on the implementation of any whitelisting applications under the DHS CDM Program, as well as identifies a time line for its implementation. If VA chooses a non-DHS whitelisting solution, VA delineates the solution selected, the associated time line for its implementation, and the integration mechanism for the CDM Agency Dashboard. The agency also lists milestones for improving VA's performance in detecting and blocking unauthorized devices and software.

Apart from the updates on Phase 1, we would also like to touch upon our progress in implementing Phase 2 of our CDM Program.

VA conducted requirements sessions with VA Stakeholders, based on the guidance provided by DHS, in order to prepare the CDM Phase 2 Business Requirements Document (BRD). The CDM Phase 2 BRD has been developed and is currently under review. VA has identified the following authoritative data sources to support the four core CDM functions within the agency.

We will continue to collaborate across VA, with DHS, and with our partners across the Federal Government in order to progress ISCM and CDM at VA. We will leverage lessons learned and update our strategies and policies in order to remain in lockstep with Federal statutes and guidance. We will look to use the latest advancements in technology, while also prioritizing security, in order to protect VA data and the Veteran.

OIS POLICY MILESTONES

Recently, we have achieved various policy milestones on the path to further advancing the VA cybersecurity program. These updates in policy allow VA to strategically leverage technologies, which will better serve the Veteran, while also confirming security is prioritized in order to protect the Veteran and VA data.

Cloud activity continues to grow across Federal agencies. In order to prioritize security and allow our stakeholders to use the latest technologies, we have established the following:

- *Cloud Security Framework*.—The use and adoption of cloud computing provide great benefits to our mission of serving our Veterans. VA's cloud security framework defines comprehensive and synchronized capabilities to identify and manage cloud security risks, protect access to our cloud environment, protect cloud applications and data, secure cloud network configuration and connectivity, oversee the physical environment security, monitor the cloud environment, and provide the ability to rapidly respond and recover from a cybersecurity event. These cloud security capabilities address security concerns, and allow VA to capture benefits from cloud computing to serve the Veteran while protecting Veteran and VA data.
- *Cloud Security Guidance*.—Our Cloud Security Guidance, which aims to provide guidelines and the minimum requirements, is intended to mitigate the risk associated with increased attack surface for cloud-based systems. Cloud Service Providers are especially vulnerable to attackers due to the value and quantity of data being stored in the cloud. Multi-tenancy increases this risk as VA will not have control of or insight into the security posture of other tenants. Due to lack of familiarity with cloud, misconceptions about the shared responsibility model, and a history of breaches in Government cloud systems due to their misconfiguration, VA shall employ cloud-centric defense-in-depth to help reduce these risks.

We have instituted VA Handbook 6500.11, *VA Firewall Configuration*, a firewall policy to cover new technologies in coordination with the Office of Cybersecurity Policy and Compliance. This policy reflects firewall configurations, which are required to comply with the provisions of FISMA and other related information security requirements promulgated by NIST and OMB. We have published VA Directive and

Handbook 6513: *Secure External Connections,* which governs the process for managing and continuously monitoring VA connections.

IT MODERNIZATION

Foundation of Modernization

Secretary Shulkin is committed to this vision and making VA a world-class organization. Whether it is from silos to collaboration, or from process to Veteran outcomes, or from guarded to transparent, we are changing the culture at VA. For OIT, that means we must innovate and modernize to provide the best services possible. Modernizing our technology plays a huge role in helping us achieve this objective. That means looking differently at how we provide services to Veterans insofar as how we streamline our approach to take advantage of new technology and industry best practices; improve the ways we deliver care, benefits, and services to Veterans; and how we embrace change and refocus on why and how we serve Veterans.

VA OIT Modernization Strategy

The mission of VA OIT is to collaborate with our business partners to create the best experience for all Veterans. OIT's three goals—Stabilize and Streamline Processes; Eliminate Material Weaknesses; and Institutionalize New Capabilities—drive our strategy and outcomes. They are enduring and will continue to frame our plans for 2018 and beyond. VA OIT approaches everything through our core values of transparency, accountability, innovation, and teamwork. Values we seek to embody, every day, in every project, and for every Veteran.

OIT is committed to VA's I–CARE (Integrity, Commitment, Advocacy, Respect, and Excellence) values and the underlying responsibility to provide the best level of care and services to our Veterans. We expect nothing less and will not tolerate employees who deviate from those core values.

Our comprehensive IT Plan is the foundation for reducing our reliance on legacy systems, and creating new capabilities for a modern VA by leveraging cloud, digital platforms, while incorporating other modern and innovative technologies such as expanded telehealth, robotics, Artificial Intelligence, mobile devices, machine learning, Blockchain, and digital services to increase access, engagement, and interoperability. Through this plan, we will stop or migrate 240 of our 299 projects over the next 18 months, and leverage a buy-first strategy—getting us out of the software development business and ensuring we are positioned to manage the influx of new technologies. We will ensure that we have end-user accessibility of these systems to be Section 508-compliant.

VA is investing in innovative solutions and industry best practices to build a stronger; more advanced IT backbone to better serve Veterans with a focus on Managing Data, Migrating to the Cloud, Improving Cybersecurity, Digitizing Business Processes, and Decommissioning Legacy Systems. OIT's five modernization priorities are built on transformation. They facilitate a modern IT infrastructure that supports OIT's vision of becoming a world-class organization that provides a seamless, unified Veteran experience through the delivery of state-of-the-art technology.

The Path Forward

We are plotting a path forward for a modern VA that seamlessly connects Veterans with the care, benefits, and services they have earned. In OIT, we are committed to investing in new and emerging IT solutions such as artificial intelligence, robotics, and self-service tools that revolutionize the way Veterans and VA employees interact with our digital framework. This commitment enables VA to continue to provide high-quality, efficient care, and services that keep up with the latest technology solutions and standards of care. The future of VA's IT modernization is rooted in eight of our key initiatives: EHRM, enterprise-wide API Management Platform, Financial Management Business Transformation, cybersecurity, scheduling enhancements, telehealth expansion, legacy system modernization, and data center consolidation.

First and foremost is our EHRM initiative. On June 5, 2017, Secretary Shulkin announced his decision to adopt the same Electronic Health Records (EHR) technology as DoD. This transformation is about improving VA services and significantly enhancing the coordination of care for Veterans who receive medical care not only from VA, but DoD and our community partners. We have a tremendous opportunity for the future with EHRM to build transparency with Veterans and their care providers, expand the use of data, and increase our ability to communicate and collaborate with DoD and community care providers. In addition to improving patient care, a single, seamless EHR environment will result in a more efficient use of VA resources, particularly as it relates to health care providers. This new EHR system will enable VA to keep pace with the improvements in health IT and cybersecurity,

which the current system, VistA, is unable to do. Moreover, the acquisition of the same solution as DoD, along with the added support of joint interagency governance and support from National EHR leadership including VA partners in industry, Government, academic affiliates, and integrated health care organizations, will enable VA to meaningfully advance the goal of providing a single longitudinal patient record that will capture all of a Servicemember's active duty and Veteran health care experiences. It will enable seamless care between the Departments without the additional step of exchanging and reconciling data between two systems that are not integrated and operate in separate environments. To that end, the Secretary has insisted on high levels of interoperability and data accessibility with our commercial health partners in addition to the interoperability with DoD. Collectively, this will result in better service to Veterans since transitioning Servicemembers will have their medical records made available to VA without any intervention.

Our second initiative supports VA's commitment to leverage our community partners and innovative technologies to give Veterans a digital experience in line with what they receive from the private sector through APIs. VA's strategic open API program called Lighthouse that adopts an outside-in, value-to-business-driven approach to create APIs that are managed as products to be consumed by developers internal and external to VA. Such an approach serves as a change catalyst, which will allow VA to decouple systems and continue to leverage its investment in various digital assets, support application rationalization, and allow it to absorb new, commercial SaaS to replace home-grown, outdated systems. This strategy calls for a clearly-defined operating model for managing the complete life cycle of APIs and will include the planning, design, implementation, publication, maintenance, and retirement of APIs as well the operation of the API Gateway platform on a VA private cloud.

The API Gateway leverages FHIR so as to enable enhanced data interoperability between both internal and external systems. API-enabled and FHIR-based solutions are easier for developers to implement as it makes use of modern web standards and RESTful architectures with more easily understood specifications. By liberating data and enhancing interoperability with FHIR, VA will be able to shift ownership of the data to Veterans and make that data more readily available for whom it is necessary. Additionally, these resources will allow for more powerful solutions to be developed which will allow for a more seamless patient and provider experience.

We released our developer sandbox in beta 2 weeks ago. We are looking for a small, initial-user group to join our developer community to make sure we follow industry best practices around tools, documentation, governance, and support workflows. As this community grows and VA releases more APIs, Lighthouse will serve as the "front door" to VA's vast data stores—giving developers access to standardized data sets they need to build mobile and web apps for our Veterans.

As part of VA's commitment to promoting interoperability and standardized data sharing through Lighthouse, Secretary Shulkin announced VA's Open API Pledge, which reaffirms VA's commitment to giving developers access to our systems through standards-based APIs so that they can build Veteran and clinician-designated applications. In exchange, we are asking health care providers to sign a pledge to work with VA to accelerate the mapping of health data to industry standards, including the current and future versions of FHIR.

Our third initiative supports VA's back-end systems and reduces our reliance on outdated legacy systems, so our clinicians and employees have the modern tools and IT support they need. VA's Financial Management Business Transformation effort is currently under way and will positively impact the delivery of all health and benefits by standardizing and improving accounting and acquisition activities across VA's enterprise. VA has an urgent need to address multiple legacy platforms used today in our finance and accounting mission critical functions. We are working to adopt and implement a commercial, cloud-hosted integrated financial and acquisitions system. This transformation effort will increase the transparency, accuracy, timeliness, and reliability of financial information. The result will be improved fiscal accountability to American taxpayers and improved care and services to our Veterans as well as transforming the Department from numerous stovepipe legacy systems to a proven, flexible, shared service business transaction environment.

Our fourth initiative focuses on bolstering our enterprise cybersecurity framework to proactively respond to emerging data threats and the evolving cybersecurity landscape. VA's Enterprise Cybersecurity Strategy will ensure that Veteran data are secure, available, and safe from cyber threats. Safeguarding Veteran information and VA data is essential to providing quality health care, benefits, and services to our Nation's Veterans.

Our fifth initiative extends to modernizing and enhancing the Department's scheduling systems. As a patient who receives treatment at both the Washington,

DC, and Baltimore VA Medical Centers, enhanced scheduling is something I am very passionate about. We are launching new digital tools that enable Veterans to schedule appointments on-line, use mobile applications to manage prescriptions, and participate in video conferences with their care providers as needed. We are also investing in solutions that give our providers a more seamless experience with the back-end scheduling tools they need to serve our Veterans. We have made strides in our scheduling tools, but we still have a long way to go. We now have VistA Scheduling Enhancement (VSE) upgrades fully implemented in 158 of 160 sites improving the interface for the schedulers so they easily view appointment times and reduce scheduling errors. Any person can now conduct their Scheduling activities at those sites using VSE. Some sites have greater utilization than others based on the level of training of users per site, which is increasing daily. We have seen on-line scheduling increase 5 times due to recent improvements; this capability is currently in place at more than 100 sites. The Medical Appointment Scheduling System is being piloted in Columbus, Ohio, and the Faster Care for Veterans Act test installs have been successfully completed in Minneapolis, Minnesota; Salt Lake City, Utah; and Bedford, Massachusetts. Last year, the Secretary launched a new access and quality tool, known as "Access to Care." This web-based site was developed for Veterans and their families to see in real time the wait times at local VA facilities, VA hospital ratings, and comparisons with private hospitals in their area. This information empowers Veterans to choose the time and place they receive their care. Not only will this website take in and process complex data, but it will make the data transparent to Veterans. We will continue improving transparency via the Access to Care site as we receive feedback from Veterans, employees, Veterans Service Organizations, and Congress.

In addition to scheduling enhancements, VA and OIT are making strides in our telehealth programs. We are expanding telehealth capabilities with hubs around the country to better service Veterans who live in rural communities or have challenges accessing VA medical centers due to their mobility. More Veterans have access to tele-mental, tele-urgent, and tele-specialty care. On March 6, 2018, the Secretary announced VA's plan to launch a Nation-wide telehealth program to help Veterans dealing with post-traumatic stress disorder (PTSD). The pilot program will connect 12 community-based outpatient clinics (CBOC) across the Nation with Veterans in need of treatment for PTSD. This program will help greater numbers of Veterans living in rural areas and will save them time and effort to travel to a VA facility that is far from their homes.

Another significant VA and OIT initiative is Legacy Systems Modernization. We are moving critical functions from outdated and difficult to sustain platforms into more modern systems that operate at lower maintenance costs. Our planned IT investments prioritize the development of replacements for specific mission-critical legacy systems, such as the Benefits Delivery Network, as well as operations and maintenance of all VA IT infrastructures essential to deliver medical care and benefits to Veterans. Investments in IT will also support efforts and initiatives that are directly Veteran-facing, such as mental health applications to support suicide prevention, modifications of multiple programs to accommodate special requirements of the community care program, Veteran self-service applications (Navigator concept), education claims processing integration consolidation, and benefit claim appeals modernization.

OIT continues its Data Center Consolidation effort to merge and close data centers at VA facilities Nation-wide. During fiscal year 2017 the team closed 24 data centers. The team plans to close another 91 by the end of fiscal year 2018. The benefits of the Data Center Consolidation effort include increased system security, reliability, and efficiency; enhanced cybersecurity; and the opportunity to introduce innovative and cost-saving technological advances to VA systems. These improvements will allow VA employees to spend less time managing the infrastructure and more time on customer-focused activities that better serve Veterans. As OIT continues to make progress in data center consolidation, VA will remain a Government leader in compliance with FITARA.

We are on an ambitious journey to become the No. 1 customer service agency within the Federal Government. By investing in innovative solutions—from technology to new ideas—we are on the right trajectory to advance toward our modernization goals and to make VA a greater choice for all Veterans.

CONCLUSION

Thank you again for the opportunity to appear before you today to address the status and progress that the VA OIT is making toward its deployment of the CDM Program and our IT modernization efforts. Throughout this modernization, our No.

1 priority has and will be always the Veteran. Ensuring a safe and secure environment for their information and improving their experience is our goal. I look forward to answering your questions.

Mr. RATCLIFFE. Thank you Mr. Blackburn.

The Chair now recognizes Mr. Garcia for 5 minutes.

STATEMENT OF DAVID GARCIA, CHIEF INFORMATION OFFICER, U.S. OFFICE OF PERSONNEL MANAGEMENT

Mr. GARCIA. Thank you, Chairman Ratcliffe, Chairman Hurd, and distinguished Members of the subcommittees who are engaging in this important discussion. I appreciate the opportunity to appear before you here today.

Although I am new to OPM, I am pleased with the transformative activities that my office is already undertaking. Since arriving, I have worked with senior staff to identify key priorities to drive our efforts to build governance processes to support our work. We recognize that OPM is an organization made up of terrific people with the mission to serve not just the Federal work force but also the American people. To successfully meet this important mission, OPM will continue to bring to the Federal Government agile, modern IT solutions that reflect its needs and leverage forward-leaning capabilities. The Department of Homeland Security's CDM Program is an important element to assist us with this goal.

As the former CIO for the State of Maryland and as an executive with over 20 years private-sector experience, I look at OPM's current posture through both a private and public-sector viewpoint. There are two main points that I think are critical to the context of the conversation we are having here today. First, you must understand that CDM is a broad approach and is continuously evolving. Every day, the malicious actors around the globe, who are equivalent to military-grade adversaries, are adapting. Therefore, as Federal agencies, we need to have the flexibility to adapt rapidly.

Second, we must strive to have CDM and similar future programs reduce the time required for the public sector to procure technological solutions. As an entrepreneur and small business owner and like our private-sector industry partners, I had the flexibility to procure and implement solutions to mitigate zero-day threats and vulnerabilities without delay. However, as a CIO for a Federal agency, I do not have that same flexibility. CDM can be tuned to enhance the abilities of agencies to procure the needed cyber defenses as quickly as possible. I feel this provides agencies the best fighting chance to stay ahead of possible threats.

As you may know, OPM is one of first agencies to fully implement CDM, and OPM completed implementation of phase 1 with the CDM dashboard fully populated in the spring of 2017. This phase focuses on managing what is on the network, to include management and control of devices, software, security configuration settings, and software vulnerabilities. For OPM, this has meant gaining greater insights to connection points within our network.

In addition, OPM has made use of CDM technologies to identify and strategically resolve potential vulnerabilities, which has resulted in better overall risk management and response. OPM is on

track to complete implementation of phase 2 in the summer of 2018, ahead of the scheduled fall 2018 target. Phase 2 focuses on the management and control of user access privileges. Phase 2 has allowed OPM to standardize the access assistance so that management of all accounts is unified and controlled through an agency governance process. Reducing the volume and scope of user access also helps OPM identify anomalies related to possible insider threat activities and prevent data loss. This is especially critical in the context of the events of 2015 because it will add additional two-factor authentication requirements to address long-standing audit findings.

OPM has been successful in the implementation of phase 1 and phase 2 due to the alignment of the technology with the agency technology strategy and life-cycle management. The use of CDM has set the stage for OPM to move into a continuous monitoring approach that enhances OPM's ability to manage its systems and continually evolve its systems to secure in real time.

Looking forward, the future should allow CIOs and CISOs the ability to move as quickly as new technologies and threats evolve. Due to the asymmetric nature of attacks, we need to consider security risks related to the increasing use of artificial intelligence, AI, by our adversaries. For CDM to be successful in the long term, it will need to continue to evolve, including the use of new ideas and concepts, such as the use of AI within the Federal networks.

I accepted the position at OPM because I truly believe in the mission of OPM because it is an agency in which great success can be achieved and demonstrated. The people of OPM are dedicated. New technology is being implemented and the agency is committed to supporting all the Federal employees who devote their lives to serving the American people.

I look forward to working with the Members of these subcommittees to continue our efforts at modernization and the evolution of the CDM Program so that it will remain a successful resource for Federal agencies.

Thank you for the opportunity to testify before you today. I look forward to answering any questions you may have.

[The prepared statement of Mr. Garcia follows:]

PREPARED STATEMENT OF DAVID GARCIA

MARCH 20, 2018

Thank you Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, and Members of the subcommittees for engaging in this important discussion. I appreciate the opportunity to appear before you today.

Although I am new to the U.S. Office of Personnel Management (OPM), having only been at the agency for about 6 months, I am pleased with the transformative activities that my office has already undertaken. Since arriving, I have worked with senior staff to identify key priorities to drive our efforts and to build governance processes to support our work. We recognize that OPM is an organization made up of terrific people with a mission to serve not just the Federal workforce, but also the American people. To successfully meet this important mission, OPM will continue to bring to the Federal Government agile, modern Information Technology (IT) solutions that reflect its needs and leverage forward-leaning capabilities. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program is an important element to assist us with this goal.

As the former chief information officer (CIO) for the State of Maryland, and with over 20 years of private-sector executive experience, I look at OPM's current posture through both a private- and public-sector viewpoint. There are two main points that

I think are critical to the context of the conversation we are having today regarding CDM. First, we must understand that CDM is a broad approach and is continuously evolving. Every day the malicious actors around the globe, who are equivalent to military-grade adversaries, are adapting. Therefore, as Federal agencies, we need to have the flexibility to adapt. Second, we must strive to have CDM and similar future programs, reduce the time required for the public sector to procure technological solutions compared to the time it takes in the private sector, which contributes to a gap in preparedness. As an entrepreneur and small business owner in the private sector, I had the flexibility to procure and implement a solution to mitigate a zero-day threat or vulnerability immediately; however, as the CIO for a Federal agency, I do not have that same flexibility to get needed tools on our network in real time. While CDM has certainly reduced the procurement time frame for cybersecurity technology, a goal should be to continue to enhance the ability for agencies to procure what they need to maintain the appropriate cyber defenses as quickly as possible. The faster agencies can procure technology, the faster technology can be implemented—which gives agencies the best chance to stay ahead of possible threats that continue to evolve and become more sophisticated.

Since coming to OPM, I have developed a vision of the top five priorities the CIO must address to successfully support OPM. Those priorities are: (1) Continue to fully mature the Risk Management Program by building on OPM's cybersecurity success to date, applying new technologies and techniques, and implementing the best practice recommendations from the Department of Homeland Security, the Government Accountability Office, and OPM's Inspector General, as appropriate; (2) work with stakeholders to provide new and innovative customer experiences through the latest technology; (3) utilize technology to reduce the investigation inventory; (4) create IT financial transparency through implementation of a standardized technology with the ability to develop a sustainable, transparent, and repeatable financial model; and (5) align the CIO organization to better meet the needs of OPM by providing a foundation for current and efficient services that will last longer than the life span of a server and that can be leveraged for the long term.

CDM supports these priorities and OPM will continue to build off of its successful implementation of CDM's Phase 1 and the continued implementation of Phase 2. As you may know, OPM is one of the first agencies to fully implement CDM, and we have benefited from the enhanced visibility into who and what is on our network so that we can more accurately and rapidly respond to potential risks. OPM completed implementation of CDM Phase 1 with the CDM dashboard fully populated in the spring of 2017 using the CDM sensors we've been deploying since 2015. This phase focuses on managing "what is on the network," to include the management and control of devices, software, security configuration settings, and software vulnerabilities. For OPM, this has meant gaining greater insights into connection points within our network, which provides us with the ability to better regulate devices connecting to the environment as well as a better understanding of what should actually be on the network. In addition, OPM made use of CDM technologies to identify and strategically resolve potential vulnerabilities, which has resulted in better overall risk management and response.

OPM is on track to complete implementation of CDM Phase 2 in the summer of 2018, ahead of the scheduled fall 2018 target for the Federal Government. Phase 2 focuses on the management and control of user access privileges. Phase 2 has allowed OPM to standardize the access of systems so that the management of all accounts is unified and controlled through an agency governance process. Reducing the volume and scope of user access also helps OPM identify anomalies related to possible insider threat activities and prevent data loss. Access for privileged users, which are users that have some administrative access to systems or data, is being enforced through a separate login mechanism. Our next step toward completion of CDM Phase 2 is to activate additional two-factor authentication enforcement features. This is especially critical in the context of the events of 2015 because it will add additional two-factor authentication requirements to address long-standing audit findings.

OPM has been successful in the implementation of Phase 1 and 2 of CDM due to the alignment of the technology available through CDM with agency technology strategy and life-cycle management. The use of CDM has set the stage for OPM to move into a Continuous Monitoring approach that enhances OPM's ability to manage its systems and continually evolve to secure its systems in near-real time.

I am also pleased with how CDM Phase 3 has evolved from offering very specific software or capabilities within certain National Institute of Standards and Technology control families to a "buffet"-style offering with software and capabilities supporting the necessary agility that Federal agencies require to meet the unique needs and goals related to their specific operations. Looking forward, OPM will increas-

ingly leverage CDM for our procurement needs to meet new challenges. We will prioritize our risk management needs and align the new technologies offered by CDM to meet our highest risks in a continuous effort to reduce vulnerabilities.

I see Phase 4 of CDM transitioning into an on-going and continuous monitoring effort that will allow OPM and other agencies to keep pace with malicious actors. For agencies to be successful, Phase 4 should allow the Federal Government the ability to move as quickly as new technologies and threats evolve. This can be accomplished through an offering of tools and services that meet the specific goals and needs of agencies and through agile procurement capabilities that allow agencies to change and adapt their tools in real time. Following best practices in Government procurement, coupled with a continued effort to survey what capabilities are available throughout the private sector, will help keep the Federal Government informed and on pace. For CDM to be successful in the long term, it will need to continue to evolve, including the use of new ideas and concepts, such as the use of Artificial Intelligence (AI), for immediate identification, response, and updates to threats. Due to the asymmetric nature of attacks, we also need to consider security risks related to the increasing use of AI by our adversaries across all sectors and how that may impact the kinds of cyber defense and tools we need.

I accepted the position of CIO at OPM because I truly believe in the OPM mission and because it is an agency in which great success can be achieved and demonstrated. The people at OPM are dedicated, new technology is being implemented, and the agency is committed to supporting all the Federal employees who devote their lives to serving the American people. Although there may be bumps in the Federal Government's journey to keep pace with potential cyber threats, I am confident we have an incredible opportunity to make strides toward a successful future. I look forward to working with the Members of these subcommittees to continue our efforts of IT modernization and the evolution of the CDM Program so that it will remain a successful resource for Federal agencies.

Thank you for the opportunity to testify before you today. I look forward to answering any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Garcia.

Mr. Cox, you are recognized for 5 minutes.

STATEMENT OF KEVIN COX, PROGRAM MANAGER, CONTINUOUS DIAGNOSTICS AND MITIGATION, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. COX. Thank you, Chairman.

Chairman Ratcliffe, Chairman Hurd, distinguished Members of the committees, thank you for today's opportunity to discuss the Department of Homeland Security's effort to secure Federal networks. I want to begin my testimony by thanking Congress for its work on the Cybersecurity and Infrastructure Security Agency Act of 2017. If enacted, this legislation will streamline the organization where I work, the National Protection and Programs Directorate, or NPPD. It will also rename our organization to clearly reflect our mission. The Department strongly supports this effort and appreciates the focus of these committees on seeing it enacted.

DHS serves a critical role in safeguarding and securing cyber space, a core Homeland Security mission. Cyber threats remain one of the most significant strategic risks for the United States, threatening our National security, economic prosperity, and public health and safety.

Over the past year, Federal network defenders saw the threat landscape they face grow more crowded, active, and dangerous. While, in many cases, our defenses have been successful in mitigating these threats, we must do more to ensure our cyber defenses keep pace of technological change and the evolving risks.

Last year, the President signed an Executive Order on strengthening the cybersecurity of Federal networks and critical infrastructure. Cybersecurity is an important component of the administration's IT modernization efforts and the administration is committed to securing the Federal enterprise from cyber-related threats.

One of the capabilities MPPD leverages to assist Federal agencies with their cybersecurity and MPPD with its mission of protecting the Federal enterprise is through a program I manage, the Continuous Diagnostics and Mitigation Program, CDM. CDM provides cybersecurity tools and integration services to Federal agencies. CDM is helping us achieve three major advances for Federal cybersecurity. First, agencies are gaining continuous visibility into the extent of cybersecurity risks across their entire network. This allows prioritization of cybersecurity actions.

Second, with the Federal dashboard, MPPD will be able to operationalize this visibility initially through improved vulnerability management. Prior to CDM, MPPD often tracked Government-wide programs in implementing critical patches via agency self-reporting and manual data calls. CDM is changing this model, enabling MPPD to immediately view the prevalence of a given software product or vulnerability across the Federal Government. All Cabinet-level agencies have their agency dashboards in production with additional assets being added on a daily basis. Additionally, the Federal dashboard currently has a quarter of Federal assets reporting to it. It is anticipated that the remaining in-scope Cabinet-level assets will be reporting by the end of April 2018.

Third, through the CDM Program, DHS is building important partnerships with other Federal agencies, including GSA, and industry to directly address the nation-state and criminal threats against our critical data in Federal networks. In the first phase of CDM, MPPD is helping Federal agencies better understand what is on their networks and better manage the cybersecurity of those assets. IT assets combined with their vulnerabilities and misconfigurations represent a significant attack surface that our adversaries target.

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.

The next phase seeks to understand what is happening on the network. By strengthening network protections and providing expanded visibility to the cloud and mobile devices, agencies will gain a more robust understanding of the events occurring on their networks and help them standardized incident reporting. The program is also beginning to plan for enhanced data protections in Federal agency high-value environments from information rights management to micro segmentation. These phase 4 initiatives will help agencies secure their most sensitive data, regardless of where it is located on the network.

Moving forward, the new CDM DEFEND acquisition strategy incorporates lessons learned from earlier stages of the CDM Program. CDM DEFEND contracts will support longer periods of per-

formance with higher contract ceilings to provide significant flexibility.

In closing, I want to assure these committees that DHS is embracing our statutory responsibility to administer the implementation of Federal agency cybersecurity processes, policies, and practices. The overarching goal of Federal cybersecurity is to ensure that every agency maintains an adequate level of cybersecurity commensurate with its own risk and with those of the Federal enterprise.

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

[The prepared statement of Mr. Cox follows:]

PREPARED STATEMENT OF KEVIN COX

MARCH 20, 2018

Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, and Members of the subcommittees, thank you for today's opportunity to discuss the state of Federal cybersecurity. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyber space, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. This past December, the House voted favorably on H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." If enacted, this bill would mature and streamline NPPD, renaming our organization as the Cybersecurity and Infrastructure Security Agency to clearly reflect our essential mission and role in securing cyber space. The Department strongly supports this much-needed legislation and encourages swift action by Congress to complete its work on this legislation.

NPPD is responsible for collaborating with Federal agencies to protect civilian Federal Government networks, as well as with the intelligence community; law enforcement; State, local, Tribal, and territorial governments; and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information sharing across the globe to stop cyber incidents before they start and help businesses and Government agencies to protect their cyber systems and quickly recover should such an incident occur. 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 information sharing on best practices and cyber threats, and strengthen resilience.

CYBERSECURITY PRIORITIES

This administration has prioritized protecting and defending our public and economic safety from the range of threats that exist today, including those emanating from cyber space. Last year, the President signed Executive Order (EO) 13800, on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. This order also emphasized the importance of accountability—clarifying that agency heads are responsible and will be held accountable for the security of their networks and systems. NPPD plays an important role in providing capabilities, services, and direction to Federal agencies.

Although Federal agencies have primary responsibility for their own cybersecurity, 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 Federal agencies includes:

- providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN", and the Continuous Diagnostics and Mitigation (CDM) programs;
- measuring and motivating agencies to implement policies, directives, standards, and guidelines;
- serving as a hub for information sharing and incident reporting; and

- providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services.

Today, my testimony will focus on one of the capabilities NPPD has to assist Federal agencies with their cybersecurity and DHS with protecting the Federal enterprise—the Continuous Diagnostics and Mitigation (CDM) program. 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.

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, which we address through Phase 2. By learning who has access to agency networks, including those individuals with privileged user access, agencies can 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.

CDM is helping us achieve three major advances for Federal cybersecurity.

First, agencies are gaining continuous visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance.

Second, with the Federal dashboard, the NCCIC will be able to operationalize this visibility, initially through improved vulnerability management. For example, the NCCIC currently tracks Government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of a given software product or vulnerability across the Federal Government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps.

Third, through the CDM program, the DHS is building important partnerships with the General Services Administration (GSA), other Federal agencies, and industry to directly address the nation-state and criminal threats against our critical data and Federal networks.

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.

Moving forward, the new CDM DEFEND Acquisition Strategy, developed in partnership with GSA, incorporates lessons learned from the Continuous Monitoring as a Service Blanket Purchase Agreements that were used in the early stages of the CDM Program. CDM DEFEND contracts have longer periods of performance with higher contract ceilings providing agencies more flexibility. This flexibility will allow agencies to modernize and standardize their security capabilities in a way that meets the CDM requirements and makes the most sense for each organization. CDM DEFEND will also support legacy and new infrastructure requirements such as cloud and mobile and will allow agencies to procure cybersecurity tools and services separately or together.

CONCLUSION

In the face of increasingly sophisticated threats, NPPD supports the Federal Government's efforts to defend our Nation's Federal networks and critical infrastructure from cyber threats. Our information technology is increasingly complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "internet of things" (IoT) and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our Nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

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

Mr. RATCLIFFE. Thank you, Mr. Cox.

The Chair now recognizes the Chairman of the Subcommittee on Information Technology, Mr. Hurd, for 5 minutes.

Mr. HURD. Thank you, Chairman Ratcliffe.

I appreciate the manner in which we are able to pursue these important issues and not worry about that silly word "jurisdiction" that I know bothers both of us.

Mr. Cox, I think DHS is doing a great job. I think you all—this is why we passed the Cybersecurity Act of 2015. This is why we made you all the bellybutton of protecting the dot-gov domain and coordinating with the private sector.

I have some basic questions. These aren't trick questions, but when it comes to the actual implementation, DHS has the tools that you are helping to implement on some of these other agencies. Is that correct?

Mr. COX. Yes. Through a series of mechanisms, contracting processes that we build with GSA——

Mr. HURD. Sorry to interrupt. I'm going to try to use my time judiciously. So an agency, do they have to pay you?

Mr. COX. It is through the budget that is allocated to DHS that we work with the agencies to fund the efforts to deploy the CDM capabilities.

Mr. HURD. So phase 1 implementation of CDM is basically free to those agencies?

Mr. COX. The idea is that we fund the foundational year, the base year of the licensing plus the first maintenance year, and then we transition the maintenance of those tools over to the agencies. In those first 2 years, we also provide integration support to help with the deployment of those tools.

Mr. HURD. Gotcha. So, basically, they are getting this for 2 years, and they have got to figure out to transition this to the O&M on their budget.

Mr. COX. That's correct. Yes, sir.

Mr. HURD. So, to me, this is ridiculous if there's any of the agencies that are not taking advantage of this in trying to implement this. So, once it's implemented and you're paying for the licenses, why would phase 2 cost money to the agency?

Mr. COX. It follows—phase 2, as well as our future phases, follow the same model. So we provide base year plus a maintenance year and then the cost to transition off for O&M to the agency, and there is integration support included in that.

Mr. HURD. So, Mr. Garcia, let me transition to you, since you have implemented phase 1 of this. What is your phase 2 cost?

Mr. GARCIA. To be entirely candid, I don't know the entire cost off the top of my head.

Mr. HURD. In general, what are you having to pay for? Because you've implemented software, right? You're just using that software in a different way. So you're using that software, first, to understand all the different nodes that you have on that network. Then, second, you're trying to figure out basically the access and credentials process and who has access to various things on that network. So it's not like you're having—nobody is implementing any new

software. So my question is: If you have people on your team that are managing the CDM tools, what is the cost to going to—from phase 1 to phase 2?

Mr. GARCIA. So, when we transitioned, we had other tools in place, and we basically sunset the tools that we had in place and adopted them. So, for OPM, it was rather seamless. We were doing the work already coming out of the 2014-, 2015-era stuff. So the costs were minimal, I mean, additional about what we were already doing.

Mr. HURD. I just want to confirm that point. So my question is for Mr. Blackburn and Mr. Everett: If you have a DHS that has the ability to fund the first 2 years of this and that this is a cost that should be taken over by your existing infrastructure and people, why is there any hesitancy of not accepting or implementing the other elements of phase 1, or why is phase 2 so difficult, because the cost is negligible?

Mr. EVERETT. Well, the phase 2 are some new tools that people are bringing in. So, look, we're a poor example, because, frankly, we're behind. We——

Mr. HURD. That's what I always liked about you, Mr. Everett; you're always straight, straight to the point. I appreciate that.

Mr. EVERETT. I don't like to second-guess because I wasn't there. I presume that my predecessors acted with the resources and direction they had. We're behind because we focused on a very small part of the Department. We are a large and diverse Department. So phase 1 and phase 2 were some different tool sets. On a small part of the Department, phase 1 is done. We have gone back and again at the direction of our Secretary and deputy secretary, and we are looking to cover all of phase 1 and then phase 2 for the entire Department.

Much like Mr. Garcia, a number of areas in our Department, they have CDM capabilities. What I mean by that is they have got tools that do those capabilities that we talk about in the phases. They may or may not be necessarily the tools that are part of those procurements. So, much like Mr. Garcia, our role right now is we are filling all those gaps, and then my goal over time would be to sunset some of those existing tools as we can, but integrate all the data back into our dashboard, which then goes back up to DHS.

But, very frankly, to get to your question, we're starting to look at right now—I think we figured we're working with DHS. We figured out the cost of filling our gaps. Then we're estimating right now—I think the number I had was a little over $8 million a year for the outyear M&O. Some of that may be absorbed because it will displace existing tools. Some of it is gaps in tools, in which case it is a new cost to us. So I'm working right now to make sure in our outyear budget, because we do have the time to put it in there, that we pay for that as a Department so that it doesn't become all the little ticky-tack stuff, but that we pay for it as a Department because it is a Departmental tool. Much like, again, the DHS approaches this as a Federal tool for the Federal enterprise, that is the direction we're trying to go.

Mr. HURD. Mr. Chairman, I apologize. I yield back the time I do not have.

Mr. RATCLIFFE. The Chair now recognizes the gentleman from Virginia.

Mr. CONNOLLY. Thank you, Mr. Chairman.

I do see votes have been called. We have one vote. Some of us are going to be going in and out.

Thank you all for your testimony.

Mr. Garcia, you're new, as you point out, but our committee certainly had—the head of OPM at the time of the breach testified before our committee, and she lost her job, frankly, over that incident. Coming in, looking at the situation, this was I think the largest Federal cyber breach ever, and it compromised somewhere between 24- and 28 million Americans' personal data. How confident are you that we've come a long way and that that kind of breach is unlikely to happen today? Are the vulnerabilities fundamentally still there?

Mr. GARCIA. To answer your question directly, I'm very confident.

Mr. CONNOLLY. You are very confident.

Mr. GARCIA. I'm very confident we know who and what is on our networks. Am I 100 percent? I don't think you can ever get to 100 percent as the landscape, when it changes, changes rapidly. But I'm as confident as I can be in the defenses we've put in place, and a large portion of that, quite honestly, has been hand-in-glove with the CDM Program.

Mr. CONNOLLY. Do you believe if the CDM Program had been in place, we would have—could have avoided or preempted that cyber attack?

Mr. GARCIA. So I thought about that question a lot, and I am not trying to evade here, but I don't know if I'm fully qualified to say that, not having been here during that time and understanding some of the complexities that were involved with my predecessors.

Mr. CONNOLLY. One of problems that we had at OPM at the time was duplicative—I'm sorry—systems that couldn't talk to each other, multiple systems, old systems, unencrypted systems. By and large, has that been addressed to your satisfaction as the new CIO?

Mr. GARCIA. By and large, I would say, yes. Could we get better? Yes. We have 100 percent PIV authentication for network access. We have micro segmentation. You can't get on OPM's networks unless we know you're on and have a valid PIV credential. Again, I think a lot of that work that we've done and what we see from the dashboard is again from the tools from CDM.

Mr. CONNOLLY. Let me just say to you: I hope part of your mission will be to continue to care for the people who had their data compromised because, as you know, that kind of data available, it could be years before someone decides to do something bad and your credit rating is damaged or someone gets into your financial accounts. So I do believe we have a sacred obligation to those people on-going to make sure they are protected, and I know you share that view.

Mr. GARCIA. I concur.

Mr. CONNOLLY. I thank you.

Mr. Blackburn, welcome again. Thank you for your service. It is always fascinating to hear your story about you're a customer. We've seen some reports in the press recently that the new electronic system has created more than glitches in some cases, denial

of care, mess-up of identity, drug protocols, and has actually interfered with urgent care or specialized care that our veterans need. Could you elaborate on that? I mean, how concerned are you about that? Is this something to be expected that is going to be ironed out, or do we have yet another fundamental flaw in a major investment in terms of veterans or Active-Duty health care?

Mr. BLACKBURN. So I'm very, very concerned and that—what you mentioned specifically was with the DOD's rollout of MHS GENESIS out in the Pacific Northwest, and I've been working very closely with that team. Stacy Cummings, who leads that team, she and I talk very frequently. We are monitoring that very, very closely to make sure we—when VA gets ready to launch our pilots, after we sign the contract with Cerner, that we won't be making the same mistakes. So there's a number of things that are going well with that, but there's also the things that you mentioned that are not going well, and we are working with——

Mr. CONNOLLY. I'm going to invite you to submit—certainly to our committee and I assume this committee as well. Mr. Ratcliffe, I don't mean to presume some reports on that because, obviously, we are concerned, and we have had some history. In the brief period of time I have left—thank you—Mr. Everett, we just had some public reports about Russian cyber attacks on our grid and power system, very alarming in terms of what it could do, and we previously had attacks on the nuclear power system and other systems around the country. Do you believe CDM is a tool that can help prevent that or detect that or preempt it? How worried should we be about the vulnerability especially of our grid?

Mr. EVERETT. Obviously, we take that very seriously. We work with our partners, the FBI and DHS, on ensuring that we work very well with the electric sector on those issues. Obviously, we have had a lot of briefings over even the last week. It is of special concern to me, of course, because we have our Power Marketing Administrations, which, for those who are not familiar, the Department of Energy, they are directly involved in provision of electricity for millions of Americans throughout the West and Northwest. So—that is one of reasons we are working with them to fill—they have a number of tools. We work very closely with them as part of Department. We are working to make sure anywhere that they do have gaps in the CDM capabilities that are out there, that we are working to fill them. In fact, I just had some of their folks in this morning and meet with them again, depending on snow, tomorrow. I will tell you they have a number of systems in place, and they are, very frankly, a bit of a challenge because they have industrial control systems and SCADA systems, which are bit unique. That's one of the areas we want to work with DHS, because you will always have those unique challenges, as broad as the Federal enterprise is, that we want to have them. But I absolutely believe the CDM tools, because they give you the visibility of what's on your network and who is on your network, absolutely will help you in that type of security.

Mr. CONNOLLY. Thank you.

Thank you, Mr. Chairman.

I do want to congratulate Mr. Blackburn for making progress on data center consolidation. We want to see more progress at DHS, and we want see that scorecard, FITARA scorecard, move up.

Thank you all so much for being here.

Thank you, Mr. Chairman.

Mr. RATCLIFFE. I want to advise the witnesses that votes have been called, but we are going to continue the hearing. So I am going to proceed with questions. I want to let Ms. Jackson Lee know that the hearing will continue if she wants to go vote and return, and actually, I think I'll take advantage of that myself and see you all shortly.

It looks like we are going to have to recess the hearing temporarily, very shortly, for a quick vote.

[Recess.]

Mr. RATCLIFFE. I am calling the subcommittee hearing back to order. I appreciate the witnesses' indulgence. Obviously, the vote schedule is beyond our control.

Having said that, I recognize myself for 5 minutes.

Mr. Everett, so DOE has its CDM dashboard up and running. Can you give us a sense of what the value is of the data that you're now realizing from Phase 1 CDM, what the capabilities are? What's different now that that's operational?

Mr. EVERETT. So we're just starting to pull the value out of that. We've got our IGC–3, which is essentially sort-of our enterprise SOC. Again, very frankly, one of our challenges is our scope of where we have CDM installed is limited at this point. It gives me visibility in—the services I traditionally have provisioned that are primarily to all our Federal employees is what it covers.

What it's doing is it is starting to give us the picture of, again, what our internal vulnerabilities look like, you know, as Kevin talked about, our actual vulnerability in patch management, start to give us a picture of what our prioritization should be about not only patching but about which systems are going to be no longer supported, which systems are out-of-date, some of those things.

The real value for us, frankly, is as we start to expand it across our enterprise to the PMAs and other folks. Again, many of our labs and sites already have the capabilities; we have not tied them together as an enterprise.

Mr. RATCLIFFE. OK. So are you lacking any authorities that would have allowed you to do that faster that you need now to sort-of roll it out on a more expedited—and take advantage of it on a more expedited basis?

Mr. EVERETT. So I think, for me, I can say, very fortunately, the answer is no.

At this point—you know, again, I report directly to the Secretary and deputy secretary, and that was changed right after I came on in August. That's been a huge improvement. I have their direct, firm push that we need to do this. They understand very well that we've got to know what's on our networks. That's the first step in some basic cybersecurity hygiene.

Mr. RATCLIFFE. OK.

Mr. EVERETT. So I've got that full authority.

Mr. RATCLIFFE. So then let me shift to you, Mr. Garcia, because you're a little further along the curve. So, same question regarding the new data or better data that CDM is providing.

Mr. GARCIA. So, again, just to echo what Mr. Everett said, was we were able to see across the spectrum. We can see end-of-life systems out there. We can see items that are requiring patches. We can see operating systems that are end-of-life. We can see the progress we make with our patch updates as well.

Mr. RATCLIFFE. OK.

So, in addition to your current role, you have pretty considerable private-sector experience. We're always trying to leverage what innovative companies are doing. Are there any short-term recommendations that you would make or could make from that experience that might speed up the deployment of CDM capabilities?

Mr. GARCIA. That's a great question. Since I've been with OPM, since October, I've been trying to think, how do we expedite things, how do we move things faster? I feel like we're always kind-of behind the eight-ball in Government deployment.

I think a lot of it has to do with the bureaucracy and trying to navigate that. I understand there's a balance that has to be reached and the need to be fully accountable for taxpayer dollars. But, at some point, I think there's got to be mechanisms that we can strike a balance that will enable us to move faster on some of these.

Mr. RATCLIFFE. So what would those milestones be that are out there that we can look for to know that we're on track, that we're getting—that we're making progress, you know, with respect to an effective structure for, you know, defending the Federal IT infrastructure?

Mr. GARCIA. Quite honestly, I think that CDM does provide that. If you look at Phase 1 and Phase 2, they're addressing a lot of the NIST controls that are in place. Phase 3 is moving toward that more agency focus, with the goal in Phase 4 to move into that continual monitoring of the network. I think those are good mile markers.

Mr. RATCLIFFE. OK.

So let me roll that into a question for you, Mr. Cox, we all want CDM to be a force multiplier for network defenders. What's the 3-year plan to get there? How do we know that we're getting there? What can I look at, as a Member of Congress with oversight, to say, hey, we're on track, or we're not on track, and hold you accountable?

Mr. COX. Certainly. I'll take that as two questions.

First, in terms of what we're looking at over the next 3 to 6 years is, with our CDM DEFEND contracting mechanism, we have the flexibility built in to work with the agencies to see what their priorities are at that point in time, be able to get teams in from the integrator that owns the contract, to help get the solutions deployed more quickly and being more nimble in terms of what the agency's needs are.

In terms of metrics, really looking at what we've accomplished so far and what we will be moving toward, is, to this point, getting the visibility across the networks, starting out looking at the numbers of assets that were reported manually. We found a 75 percent

increase in terms of the total number of assets once we got automated tools into the environment. From a cost-savings standpoint, by being able to do volume purchasing of the tools, we found that we achieved savings upwards of 70 percent off of IT Schedule 70.

In terms of where we're headed in being able to measure the mission impacts of CDM, we want to be able to get full visibility both at the agency level for the agencies as well as at the Federal level; and then be able to see what their overall cyber hygiene is, their security posture; and ultimately be able to help manage, for the agencies at the agency level and us at the Federal level, the risk across the Federal enterprise.

Mr. RATCLIFFE. Terrific. Thanks very much.

My time has expired. The Chair now recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Mr. Chairman, thank you. Thank you for this joint hearing.

I thank the witnesses for being instructive and insightful. I think we have a lot on our plate. Certainly, Mr. Cox, the areas that you deal with is of particular concern, and certainly the Office of Personnel Management. We're delighted that Veterans Affairs is getting on track.

But let me recite what I've done for a number of years. Just a historical perspective. This committee was included in something called Transportation Security and Infrastructure, so we began talking about these issues almost a decade ago. We're probably behind, but I'm glad to see where we are today. So I'll pose some questions initially and then—some pointed questions, but I think we've made great strides.

I emphasize a point that I wanted to make, is that we have a small percentage of the cyber, and most of it is in the private sector. A lot of that impacts Government agencies. I think that the more we are engaged—I introduced legislation that was passed—and I thank the committee—that dealt with zero-day events. Part of it was the consulting with the private sector on what might be helpful to them and what might be helpful to you that may be Classified.

So I would ask this question. As you know, one of the challenges with Federal cybersecurity is that new technologies are being developed much faster than the Federal procurement cycle allows. What should we be doing to make sure that the CDM Program is flexible and agile enough to keep pace?

Why don't I—and I'd appreciate pithy answers. I'm trying to get to all of you. Why don't I start with Mr. Cox and then go to Mr. Garcia with OPM because of the unfortunate major snafu impacting our Federal employees.

Mr. Cox.

Mr. COX. Yes, Congresswoman. We've approached the ability to bring on new technologies, new innovations more quickly in two ways.

First, through the CDM DEFEND task order. By awarding a long-term task order of 5 to 6 years, it enables us to continue to issue requests for service to that integrator for different types of technology, different types of need more quickly, rather than having to recompete a new contract.

Second, through our approved products list, we have accelerated the pace at which vendors, industry can submit new products to the approved products list. On a monthly basis, vendors can submit those to us. Working with our staff, we assess those quickly, and then, if the products meet the criteria, they're quickly added. That enables agencies to get to those products more quickly.

Ms. JACKSON LEE. Mr. Garcia.

Mr. GARCIA. Thank you for the question.

So I think the focus for us in coming out of the events of 2014 and 2015 was, how do we—if we need to buy something to address a zero-day event, we need a vendor, we need a service, we need software, we need hardware, how do we shorten the procurement time to bring these tools to bear as quickly as possible?

Ms. JACKSON LEE. Absolutely.

Mr. Garcia, I've got you right on the spot here. Does this either flexibility or attentiveness to moving forward include and embrace small, minority-, and women-owned businesses in the context of how the Federal Government utilizes so they're not shut out of the door because of their size?

Mr. GARCIA. That's a great question. So, as a former 8(a) program member, I would say "absolutely" to that question.

Ms. JACKSON LEE. That they have the opportunity?

Mr. GARCIA. Absolutely.

Ms. JACKSON LEE. Let me go right to Mr.—for the Veterans Affairs, Mr. Blackburn. Thank you for your service.

We lived in a nightmare as our veterans were either dying or not being able to get served. We know that it is certainly an old agency, and it deals with older patients who deserve our honor and respect.

What have you been able to do to cure that devastating experience that veterans have had, languishing in hallways waiting on doctors or not getting their doctor appointments?

Mr. BLACKBURN. Well, that nightmare is why I joined after 2014. I was as shocked and disgusted as anybody.

We've really pushed hard on shortening the wait times so that we now have same-day access in all of our sites. We've really doubled down on customer service, self-service tools for—I schedule my appointments now using an on-line tool.

So we're using technology. We're staffing. We're focusing on the biggest problems to make sure that that never happens again.

Ms. JACKSON LEE. Two last questions, which I'd like all of you to answer, is: What do you view as the greatest promise on the CDM for the Federal network?

But as you answer that, please—I've introduced another piece of legislation to improve the cyber professional staff for the Federal Government. If that would be helpful to you, you might acknowledge that.

But the final question—that question is No. 1, about what's the greatest promise. The other one is, in the backdrop of this hearing, we have an unfortunate discovery of the entity with Facebook, Cambridge, and the misuse of millions of emails or data of Americans.

My question would be—we don't want to be in that position. What relationship should the Government have?

We use these tools—Facebook, Google. I would hope we never acknowledge that they've gotten bigger than us, in terms of being able to overrun what are legitimate responsibilities of the Government to protect the American people.

So if you would answer how our interface would be with these giants. Because we have the most and highest responsibility, and that is to the American people.

Do you want to start, Mr. Everett?

Mr. EVERETT. Yes, ma'am.

I think, on your first question, aside from just the value of the tools themselves, I think one of the greatest promises, long-term, for the CDM Program ultimately should be the ability for us at the Federal enterprise level to start to share information together. I think that's just an opportunity that we have not taken full advantage of.

I understand it's part of the purpose of DHS being given that role as a coordinator that we as a Federal—you know, that we're all seeing different perspectives of the cyber threat, and I think that CDM, longer-term, provides an avenue that we can share that information across the entire Federal enterprise to help protect each other.

As to your other question, I would just say I think that's a challenge not just for us in Government but certainly culturally, is helping people understand the privacy issues and how that ties into our security.

You know, as somebody who did this and used to talk to people in the private sector and try and give some training, most of us, even as professionals in this, very often don't really think about the implications of some of the tools we use on our privacy and then what, in turn, that does to our security.

So I think that probably takes longer, looking at across the Federal enterprise and making sure that privacy is a part of our discussion of security. Because they do—you know, the bad guys typically want to misuse those kind of tools to get into our networks and do other things. So we need to tie those together.

Ms. JACKSON LEE. Thank you.

Mr. Blackburn.

Mr. BLACKBURN. To me, the promise of CDM, it's really moving from a reactive posture to a proactive posture.

A little less than a year ago, the WannaCry virus targeted us as well as many others, and we, luckily, had the patches in place and fared well, but the U.K. health care system, for example, not so much. We don't know what the next threats are going to be. We have to stay on top of that, proactive, and find those before they hurt us.

On the second question, I agree completely with Mr. Everett. What I would add on to that is, you know, the relationship with those giants—the Facebooks, the Googles—and making sure that we are constantly sharing the best practices and making sure that we are incorporating those things. But also, to your other point that you made a little bit earlier, which is, those companies were small and innovative. A lot of the great companies that have created such great platforms have come out of that small, agile, inno-

vative—so make sure that we're also providing opportunities for those types of companies, as well, to induce, like, the best practices.

Ms. JACKSON LEE. Yes? Mr. Garcia again.

Mr. RATCLIFFE. The gentlelady's time has expired, but, Mr. Garcia and Mr. Cox, weigh in very quickly, if you can.

Ms. JACKSON LEE. Thank you, Mr. Chairman, for your indulgence.

Mr. GARCIA. So, to the first question, promise, I'd have to agree with my colleagues. I think sharing, along with reciprocity and interagency agreements, if we could standardize these things, I think it would do a great value to the Federal Government.

As to the second question, I feel a bit uneasy to answer the question due to the fact I'm not fully aware of what's Facebook's public data policies with their open data and what agreements they had in place. I don't know that it's really fair for me, as an OPM and representative of the Government, to really—to comment on that without that knowledge.

Ms. JACKSON LEE. Thank you.

Mr.——

Mr. COX. Yes, Congresswoman. What the real key for us, to echo what Mr. Blackburn said, is to get from a reactive stance to a proactive. We want to get out in front of the threat. We want to take the low-hanging fruit out of the equation and be able to enable these agencies, as well as all agencies, with the visibility of their networks, to be able to see where the threat is and shut it down.

Again, like Mr. Garcia said, I don't feel that I'm in a good position to comment specifically on the Facebook case. But I would say that it is important for us to continue to build our partnerships with industry, to interact with them, learn what they're doing. We can share our lessons as well. We, as a Nation, continue to get better.

Thank you.

Ms. JACKSON LEE. I yield back the time. Thank you, Mr. Chairman.

The Chairman. I thank the gentlelady.

The Chair now recognizes the gentleman from Nebraska, Mr. Bacon.

Mr. BACON. Thank you, Mr. Chairman. I appreciate it.

Thanks for being here.

I've got a question for Mr. Cox.

The CDM, will you be looking at it at DHS from an enterprise-wide DHS, or will it be all the sub-agencies doing CDM? How do you integrate that? So I'm sort-of nosy on that.

Mr. COX. Certainly. The idea is that each component or operational division in each agency will be able to have the visibility for their particular mission area and their particular component.

So, specifically with DHS, we're working—our program office is working with the DHS Office of the CIO, similar to as we work with the agencies here, to help them get the solutions out, help them build the partnerships with the components, so that they, the CIO's office, get the visibility across DHS, but at the same time the components within DHS get that same visibility for their component space.

Mr. BACON. Uh-huh. Will you have enterprise-wide visibility and see the integration or get the synergy out of that?

Mr. COX. That's correct. So, while each component will have visibility for their component, that information is aggregated up at the object level, so the Office of the CIO will be able to see individual devices, individual systems.

Mr. BACON. Right.

Mr. COX. Then what we're doing from the agency level up to the Federal level is summarizing that data. So, at the Federal level, what we're seeing is a summary view but with enough information that we can work with the agencies to respond to particular issues or incidents.

Mr. BACON. Does this take advantage of commercial off-the-shelf technology pretty readily?

Mr. COX. It does. That's a core principle of the program. We didn't want to do a lot of customized builds here. We wanted commercial off-the-shelf, that the product could be put in place quickly, the agency could learn it quickly and be able to get value from it immediately.

Mr. BACON. Right.

One question for you, but it may be applicable for everybody, but I'll just get your perspective. Will the automation help you reduce some manpower requirements by this? Do you get some savings where you can redirect people?

Mr. COX. That's exactly right. That's the idea, is that we change these manual processes that we've followed for so long, get automated data so we can make better decisions more quickly. Then those folks that were doing that manual assessment work before, we can reassign those efforts to security operations and being able to help identify the threat and get in front of it.

Mr. BACON. This next question really is for you and Mr. Everett. One of the things that disturbs me most—and I'm not sure how applicable right now it is to CDM, but I'm going to give you a chance to touch on it—is the vulnerability of our energy grid. I'm not sure which portfolio that falls in.

I was afraid to talk about it too much until yesterday. Now, all this data has been released saying just how vulnerable our energy grid is.

I mean, it was thought, because there's so many—you know, it's such a fragmented system out there, how would the Russians and Chinese devote the manpower to get in there and really attack this? But with yesterday's release, we see they are trying to do that.

How does CDM help either one of you go after this huge threat? Does it facilitate or—does it directly help or indirectly?

Mr. COX. I'll start and provide the program's perspective and then turn it over to Mr. Everett.

Our idea is that we want to provide Mr. Everett and the rest of the agencies the visibility of their network, be able to get vulnerabilities quickly patched, get the systems properly configured to reduce the likelihood that an adversary can easily get into that system.

We then want to help the agencies get visibility across their network so that they can detect any attacks to their network, any threats in their network, and address them quickly.

Mr. BACON. But we wouldn't be able to help if the Russians or Chinese were attacking our energy grid separate from the network right now. Would that be—is that an accurate statement?

Mr. COX. The idea is that, if any adversary is trying to get in on the network, that we want to be able to ensure the agencies have full visibility of their network to see where that attack might be coming in. Even if it's coming in from a third party, we want to be able to see where that interface from that third party is coming into the agency network so that the agency can properly respond and quickly respond to shut it down.

Mr. BACON. Thank you.

Mr. Everett.

Mr. EVERETT. So I think I'll actually start—obviously, our Department is very focused on that. As a sector-specific agency, we work very closely with our colleagues at DHS. You know, while my focus is primarily our internal cybersecurity, the fact is I have part of the electric sector and the electric grid in our Department through our Power Marketing Administration. So it is very critical to us, and we try and leverage that understanding and knowledge in our work with the sector.

I'll tell you, frankly, almost even a little more practically, one of the values of things like CDM is our credibility with the sector only goes as far as our actual capability. So, to the degree that we're doing it well as a Federal Government, then we have a leg to stand on when we go and talk to the sector and other folks. To the degree we don't, they're likely not going to take us very seriously.

That's really how we're trying to approach it at DOE, is that we're trying to make sure that if we're doing it well, then we have something to say and something of value to bring out to the private sector, which is important. So that's one of several reasons that we take this very seriously.

We think that our experience with tools like CDM, we want to be able to then sit at the table with them and share that. Because we do think tools like CDM, they are relevant to the private sector, maybe not as to the program itself, but the capabilities, the practices, and experience are very relevant, and we think they'll help.

Mr. BACON. Right.

I'll just close, because I know we're out of time, and just say I've known about this for a while, the vulnerability of our energy grid, and I think it's very alarming. I think it's—the next December 7 won't be airplanes with torpedos coming at Pearl Harbor. It's going to be triggered with an attack on our energy grid, with rolling blackouts and chaos.

So I just—you've got a tough job, but I look forward to supporting you in this effort, because we've got to start working on the resilience of our energy grid. So I appreciate hearing the connection with CDM and this threat to us.

Thank you.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for your testimony here today.

Mr. Cox, if I could start with you, the report to the President on IT modernization notes that CDM has not sought to address cloud-hosted systems and that a challenge in implementing CDM capabilities in a more cloud-friendly architecture is that security teams and security operations centers may not necessarily have the expertise available to defend the updated architecture.

Do you view CDM as having applicability to cloud architectures, or will it continue to focus on on-premise networks?

Mr. COX. Congressman, yes, indeed, we want to be able to ensure the agencies have visibility, wherever their data is, to that data, how it's being used, how it's being protected. So, as we move into Phase 3 of CDM in understanding what's happening on the network, we want to ensure we're providing the agencies capabilities to not only get on-premise visibility of their data and their networks, but wherever that data is, whether it's out in the cloud, whether it's on a mobile device, wherever it's stored or used. So we want to bring that visibility into their dashboard visibility as well as at the Federal level.

Mr. LANGEVIN. OK. Thank you.

So there have been many reports about sluggish adoption of CDM tools and capabilities.

Mr. Cox, what are the persistent obstacles to agency adoption of CDM, and what is DHS doing to overcome those obstacles?

Mr. COX. Yes, sir. One of the things we saw with the Phase 1 and Phase 2 task orders is that we built those with very defined runways. In the case of Phase 1, it was a 3-year task order. In the case of Phase 2, it was a 2-year task order.

What we saw coming in and working with the agencies is that we were coming in and they had other priorities on their plate, and so we had to, within the bounds of our task order, work to get our tasks scheduled really quite quickly. So it was a burden on the agency to make adjustments, get the resources out to get the work done.

As you can see, we've made significant progress working with the agencies to get the work done, but we've learned from that lesson. So, as we've built out our new contracting approach, CDM DEFEND, we've worked to build in longer runways, we've worked to build in more flexibility, keeping things focused on a requirements basis, and then working with the agencies to look at different ways to meet those requirements, whether it was through the deployment of a new technology or perhaps with a technology they already have in place, where we can bring the visibility into their dashboard.

Mr. LANGEVIN. OK. But are there additional authorities that you need or additional assistance required from OMB to effectively implement the program?

Mr. COX. Yes, we're working with OMB quite closely, taking a look at the OMB memorandum that was put in place in support of CDM. They are working to update that. So they are supportive of the program and continuing to move it forward. So I think we've got a good direction there.

Mr. LANGEVIN. OK. That's good to know.

I appreciate the conceptual approach of CDM's phases. However, can I ask, is there a reason they aren't being pursued in parallel? For instance, it seems that Phase 4, focusing on data protection, could be implemented at the same time as Phase 3. Is there any technical or programmatic reason beyond budget and human resources why it's not being pursued in parallel?

Mr. COX. It's a good point. The way we've constructed CDM DEFEND, it's so that different tasks can occur in parallel, whether they be Phase 3, Phase 4, whether it be bringing some additional things that were out of scope in Phase 1 and 2 into scope and making sure that that can be done.

Why we focus now on Phase 3 is we've been building up the programmatics around that. We are currently working with our sister staff, Federal Network Resilience, to do proofs of concept of the Phase 4 technologies, working with the high-value asset environments. Then our aim is to quickly benefit from the outcome of those proofs of concept so we can begin the Phase 4 work in parallel to Phase 3.

Mr. LANGEVIN. Phase 4 is only a pilot, from what I understand. Is that right?

Mr. COX. At this point. Then we will work——

Mr. LANGEVIN. Why is that?

Mr. COX. We have certain programmatic actions we need to take within our Department to present the life-cycle cost estimates for the program, other important programmatic capabilities around showing that we're ready and able to fund and execute Phase 4 work.

So we're currently working that, with the idea that by the end of the summer we will go through that programmatic review within the Department.

Mr. LANGEVIN. OK.

I'm having technical difficulties with the mike here, but I also serve on the Armed Services Committee and have seen DOD's attempts to implement enterprise-wide cybersecurity acquisition programs.

How are you coordinating best practices with them, and what lessons have you learned from their attempts and newer programs, such as DOD Endpoint Security Solutions and Comply to Connect?

Mr. COX. We are currently working with our colleagues within DOD. We have a meeting scheduled next week, we've had conversations prior, to able to share our lessons learned on the capabilities that we're deploying, similar to what they're looking at, learning the lessons from the Comply to Connect implementations within DOD. That's part of the innovation, new technology we want to look at across the Federal Government—the Comply to Connect technologies, software-defined networking, zero trust networks, et cetera.

So we are building that partnership up so that we can share back and forth our best practices, lessons learned, et cetera.

Mr. LANGEVIN. Very good.

Thank you all. I appreciate the answers.

I have some additional questions that I'll likely submit for the record unless we do a second round, but other than that, Mr. Chairman, I yield back the balance of my time.

Mr. RATCLIFFE. I thank the gentleman.

I want to thank Chairman Hurd and Ranking Member Kelly from the Oversight and Government Reform Subcommittee on Information Technology for conducting this joint hearing with us.

I want to thank, certainly, all of the witnesses for your very insightful and valuable testimony today.

I want to thank the Members for their questions.

As you just heard, some Members of the committee will have additional questions for some of the witnesses, and so we'll ask you to respond to those in writing. Pursuant to committee rule VII(D), the hearing record will be open for a period of 10 days.

Without objection, the subcommittees stand adjourned.

[Whereupon, at 4:16 p.m., the subcommittees were adjourned.]

APPENDIX

QUESTION FROM CHAIRMAN WILL HURD FOR MAX EVERETT

Question. Once maintenance costs transition from DHS to your agency, how much do you anticipate spending per year to sustain CDM?

Answer. The 2019 budget includes $185,712 for the Department's CDM maintenance costs at the current level of maturity. The Department is working to catch up with CDM Phase 1 and 2 requirements. The Department will update operations and maintenance cost estimates during the DHS CDM DEFEND Request for Service (RFS) processes, which commenced with a recent kick-off meeting.

QUESTIONS FROM RANKING MEMBER CEDRIC L. RICHMOND FOR MAX EVERETT

Question 1. In January, we held a hearing with CDM contractors, who told us that one of the challenges with implementation was the lack of dedicated personnel with the expertise necessary to use CDM technologies and take full advantage of their benefits. Is there a need within your agency for more training or more cyber personnel to deploy CDM tools?

Answer. Training and skill levels for cybersecurity staff are significant issues across both the Federal enterprise and the private sector, and this is particularly challenging with CDM. We are working aggressively to develop the means to better recruit and retain skilled cybersecurity Federal employees and contractors, both internally and in coordination with the administration's cybersecurity workforce efforts. We believe we will continue to face cybersecurity staffing challenges because of the high market demand for cyber resources in general, as well as the higher salaries available in the private sector. In concert with training and recruiting, we believe our path forward must focus on:

a. *Automation*—CDM and other automated tools let machines help lessen the requirement for manual intervention, allowing for the more efficient allocation of cyber resources.

b. *Modernization*—Cybersecurity must be built in from the moment the planning and implementation process for any new system or program begins, and it must be incorporated at every level, from the design to the user interface.

Question 2. Last week, DHS and the FBI released an alert describing an extremely sophisticated, deliberate, and successful operation by the Russian government to hack into the industrial control systems of energy providers. In your testimony, you mention some fairly alarming "gaps" that "exist across the DOE enterprise," including the National Nuclear Security Administration, the National Labs, and individual plants and sites.

How do you reconcile this, in light of what we know about how forcefully foreign actors like Russia are targeting U.S. energy?

Answer. The Department and our National Labs were very familiar with the information released, which we had previously shared with the private energy sector in our role as Sector-Specific Agency.

The Department has initiated a broad, comprehensive, and multi-phase review of the Operational Technology cyber strategy and capabilities across the Department. This approach is designed to leverage resources from across the Department's program offices and labs to identify gaps and implement requirements for improvements to monitoring and response to attacks on these systems, which will inform both the defense of our Federal systems and our ability to inform and support the energy sector. Additional phases will address the broader need for a strategic approach to advanced operational technology security solutions across the hardening, detection, and response functions.

The Department is diligently working to identify and remediate gaps that exist in our capability to detect and defend against hostile actors. We are pursuing a number of avenues in this regard, including implementation of CDM tools; focusing

our integrated Joint Cybersecurity Coordination Center (iJC3) efforts to provide better enterprise-wide cybersecurity information sharing; building enterprise incident response teams capable of responding to threats that include the Operational Technology in place at our Power Marketing Administrations and other sites; and enhancing and implementing more mature enterprise risk management to facilitate prioritization of our cybersecurity efforts based on metrics. We believe the Department's capability to execute a best-in-class cybersecurity program will enhance our ability to work with and support the energy sector in the face of expanding threats.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR MAX EVERETT

Question 1a. For your agency, is there any senior cybersecurity leadership positions that remain unfilled?

Question 1b. If so, how has that complicated your ability to move forward with CDM and other information security initiatives?

Answer. The Office of the Chief Information Officer currently has only a small number of positions unfilled. At this time, the Deputy CIO for Cybersecurity position is occupied in an acting capacity—but that has only been the case for approximately 1 month and we are actively recruiting to fill that position. In addition, we are coordinating with other offices across the enterprise to assist with their hiring efforts to fill cyber leadership positions, including to meet new requirements that are forthcoming from the planned Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

Despite the limited number of unfilled roles, I have determined in my 9 months as CIO that there are staffing challenges my office faces as we work to mature and expand our enterprise cybersecurity program. We are now in the process of identifying additional Federal positions to provide the customer service, oversight, and accountability necessary to ensure a sustainable cybersecurity posture for the Department. In some cases, critical roles have been filled by contractors that I believe Federal employees should occupy. Contractors provide flexibility and access to unique and changing subject-matter expertise, but in certain cases a Federal employee is needed to provide customer service, oversight, and accountability to critical activities.

Additionally, given the diverse missions and locations of critical Departmental offices and functions, the IT leadership and cybersecurity staff in the Department's program offices and sites are often even more critical to our cybersecurity efforts. I am working to ensure that these other cybersecurity professionals have an appropriate reporting structure across the Department's program offices.

QUESTION FROM CHAIRMAN WILL HURD FOR SCOTT BLACKBURN

Question. Once maintenance costs transition from DHS to your agency, how much do you anticipate spending per year to sustain CDM?

Answer. CDM Phase 1 and 2 capabilities are scheduled to be fully operational by 3d Qtr. of fiscal year 2019. VA just began participation in CDM Phase 3. CDM-related costs in 2019 are estimated at $48.6 million to support licensing, maintenance, and operations of deployed equipment. The exact cost is still being confirmed as DHS continues to fund various aspects of the CDM program, including hardware, software, and operations and maintenance support. The details for the long-term operation and transition costs associated with Phase 2 and 3 capabilities are still being determined.

QUESTION FROM RANKING MEMBER CEDRIC L. RICHMOND FOR SCOTT BLACKBURN

Question. In January, we held a hearing with CDM contractors, who told us that one of the challenges with implementation was the lack of dedicated personnel with the expertise necessary to use CDM technologies and take full advantage of their benefits. Is there a need within your agencies for more training or more cyber personnel to deploy CDM tools?

Answer. VA continues to deploy CDM Phase 1 and 2 capabilities using VA and DHS resources. Final implementation is currently scheduled for 3d Quarter fiscal year 2019. As appropriate, VA personnel receive training to perform their designated role and function. Once trained, the DHS contractor and VA transition functions in a manner that minimizes operational impacts. VA is also participating in the Phase 3 tasks, with plans to participate in Phase 4. Throughout VA's CDM experience, we have managed resourcing requisite to the requirement and trained staff as required. If available, VA could benefit from additional training techniques and services to further augment existing training efforts and to fill CDM supporting positions in support of all CDM Phased deployments.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR SCOTT BLACKBURN

Question 1a. For your agency, is there any senior cybersecurity leadership positions that remain unfilled?

Question 1b. If so, how has that complicated your ability to move forward with CDM and other information security initiatives?

Answer. At this time, a key role in cybersecurity leadership that is currently unfilled is the Deputy Chief Information Security Officer for Policy & Strategy which is held by an acting official. VA is currently reviewing candidates to select a permanent official for this role, however, this selection process is in the early stages of review. VA remains committed to implementing the CDM program activities. The CDM program has continued to be a priority of the agency and implementation activities have continued while those leadership roles have been held by acting officials. The CDM program has remained a top priority by coordinating with relevant leaders across participating agencies and support resources to make sure the CDM mandate is satisfied.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR SCOTT BLACKBURN

Question 1. How extensive are the cybersecurity staff and skills shortfalls at your agencies, and how are they affecting your implementation of CDM?

Answer. VA is currently in the process of transitioning responsibilities for CDM services, either through existing VA staff or other support resources. With the ongoing transition, VA is still in the process of confirming gaps in cybersecurity staff skills necessary to sustain and operate the CDM capabilities that are implemented. VA is developing a plan to address those gaps while working on the transition from DHS to VA.

Question 2. One of CDM's objectives is to replace manual, periodic, and time-intensive system authorizations with an on-going process for automated assessments and continuous authorization. Is that process working, and are manual authorization processes truly going away?

Answer. VA deployed a commercial Governance, Risk, and Compliance tool during fiscal year 2013 that initiated automated assessments and supported automatic reviews for continuous authorization. VA was able to move a purely manual assessment process to one that allowed for the automatic collection of data through tools, services, and capabilities already deployed in VA that report back compliance deficiencies and vulnerabilities across millions of VA assets. In order to expand the effectiveness of the continuous authorization capabilities, VA will deploy the Enterprise Mission Assurance Support Service (eMASS) tool used by the Department of Defense (DoD). eMASS will not only allow greater delivery of automated assessment and authorization processing, but will expand visibility for both VA and DoD into joint and partnered systems' authorizations by each respective agency.

Manual processes, to the extent possible, will be replaced by better use of compliance data, aggregated enterprise-level control reviews, and the ability to provide enhanced system-level reporting at an enterprise view. While some manual processes cannot be completely eliminated, VA will always look for automated processing capabilities where possible to replace manual requirements.

Question 3a. CDM represents a large investment of dollars and time. I would like to understand how we will know that investment has been successful, in terms of improved security across the dot-gov domain. What metrics are you using to measure whether your cybersecurity programs have actually improved your agency's security posture?

Answer. CDM automates the scanning of VA's infrastructure to identify any hardware or software that is outside the National Institute of Standards and Technology (NIST) and VA security standards, that is, any vulnerability. The control values that alert the dashboard to any such vulnerability are those standards and are built into the tool. Those are the metrics that measure VA's security posture. As vulnerabilities are identified, VA implements plans of actions and milestones to remedy them. Therefore, it is the CDM dashboard itself that will report VA's progress to improve the agency's security posture.

Question 3b. How are you employing red teams to test the successful implementation of your cybersecurity defenses?

Answer. VA has been leveraging DHS, National Cybersecurity Assessments and Technical Services (NCATS) team for the past 2 years in conducting an annual Offensive Security Assessment (OSA) of VA's implementation of cybersecurity defenses. The assessment gives the organization the ability to respond to a real-world attack in a controlled manner, with limited number of VA trusted agents aware of the full attack details. The OSA assesses VA's people, processes, and technology by

emulating various Advanced Persistent Threats (APTs) and measures our cybersecurity response.

QUESTION FROM CHAIRMAN WILL HURD FOR DAVID GARCIA

Question. Once maintenance costs transition from DHS to your agency, how much do you anticipate spending per year to sustain CDM?

Answer. OPM anticipates initially spending approximately $8 million annually to sustain the CDM Phase 1 capabilities, once the maintenance costs are transitioned from DHS.

QUESTIONS FROM RANKING MEMBER CEDRIC L. RICHMOND FOR DAVID GARCIA

Question 1. In January, we held a hearing with CDM contractors, who told us that one of the challenges with implementation was the lack of dedicated personnel with the expertise necessary to use CDM technologies and take full advantage of their benefits. Is there a need within your agencies for more training or more cyber personnel to deploy CDM tools?

Answer. OPM has dedicated personnel with the expertise necessary to use CDM technologies. However, as threats continue to evolve this will present additional challenges and agencies will need to make certain that the Federal technology and cybersecurity workforce is available and properly trained to meet such challenges.

Question 2a. The DHS Inspector General recently released a report finding a number of information security vulnerabilities at DHS, including some NPPD systems that were operating without proper authorization. What is the status of DHS's own implementation of CDM? Has the Department fully deployed Phase 1 technologies?

Answer. OPM defers to DHS to discuss its own implementation of CDM.

Question 2b. Might CDM adoption have been easier or more efficient with a Department-wide cybersecurity strategy in place, as was required under legislation I authored in 2016?

Answer. OPM defers to DHS to discuss its own implementation of CDM.

QUESTION FROM RANKING MEMBER ROBIN L. KELLY FOR DAVID GARCIA

Question. During Phase 1 implementation of CDM, many Federal agencies discovered that they had greatly underestimated the number of devices on their network and, as a result, the planned-for CDM deployments would be inadequate to service their larger networks. Indeed, DHS has publicly acknowledged that it identified 44 percent more devices on Federal civilian networks than originally projected, leading to significant gaps in coverage. Filling these gaps should be a significant priority for DHS and its civilian agency partners as CDM proceeds. What risk does the current level of coverage present and how soon will the identified gaps be filled?

Answer. OPM accurately estimated the number of devices on the OPM network during Phase 1 implementation of CDM. In addition, OPM is working with DHS to improve and enhance the end-to-end protections where gaps were identified in the overall solution.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR DAVID GARCIA

Question 1a. For your agency, is there any senior cybersecurity leadership positions that remains unfilled?

Question 1b. If so, how has that complicated your ability to move forward with CDM and other information security initiatives?

Answer. Currently, there are no senior cybersecurity leadership positions that remain unfilled at OPM. OPM was one of the first agencies to fully implement CDM Phase 1 with the CDM dashboard fully populated in the spring of 2017 using the CDM sensors we've been deploying since 2015. In addition, we are finalizing the implementation of CDM Phase 2.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR KEVIN COX

Question 1a. What is the time line for the CDM program office to produce the capability requirements for Phase 4?

Answer. The Continuous Diagnostics and Mitigation (CDM) Program is developing the Phase 4 capability requirements and expects to have them completed by the first quarter of fiscal year 2019.

Question 1b. When is the earliest an agency could have moved through all CDM phases?

Answer. The program is beginning Phase 3 and starting Phase 4 pilots in fiscal year 2018. Phase 3, which includes cloud and mobile continuous visibility, is expected to run through fiscal year 2021. Phase 4 will be focused on providing enhanced data protection for high-value asset (HVA) environments and is expected to run through fiscal year 2023. The date by which an agency could move through all CDM phases is dependent on the size of the agency, its total number of HVAs, its readiness and prioritization for CDM solution deployment, and overall funding. We plan to begin deployment of Phase 4 data protection capabilities in fiscal year 2019 for an initial set of agencies who are ready for the capabilities and fall within our budget. The time line to fully deploy Phase 4 is dependent on the agency's specific requirements, readiness, and CDM funding.

Question 1c. What is beyond Phase 4?

Answer. The CDM program includes activities required to keep pace with technology advances over the life of the program. The Department of Homeland Security (DHS) is still developing the future strategy for the CDM program to ensure that the program evolves after the currently defined four capabilities are deployed. The most appropriate path forward is to stay in front of the cybersecurity threat and support the agencies as threats and technology evolve. As part of this consideration, the program is now transitioning from the phase model to a capabilities-based model that anticipates threats. By shifting to a capabilities focus, the program can address specific new cybersecurity capabilities as they develop throughout the life cycle of the program.

Question 1d. Are there plans for a long-term strategy to ensure CDM is a platform for an effective cybersecurity posture in the next 3 to 5 years?

Answer. In the fiscal year 2018 President's budget, additional funding was given to the program to speed up the deployment of mobile asset tracking and cloud asset tracking—both previously defined as Phase 3 activities starting in fiscal year 2019 and fiscal year 2020. Funding, however, is not the only factor in the speed at which CDM is deployed. DHS is actively working with agencies to identify where Phase 3 efforts can be adopted more quickly based on agency readiness and where Phase 4 pilot efforts can be accelerated.

Question 1e. Has DHS considered accelerating the roll-out and adoption of the capabilities in Phases 3 and 4, similar to what was done with the Einstein E3A initiative?

Answer. Response was not received at the time of publication.

Question 2a. How can CDM be leveraged to better understand the security posture of High-Value Assets?

Answer. When and where possible, the Continuous Diagnostics Mitigation (CDM) Phase 1 tools are deployed in the High-Value Asset (HVA) environments to gain continuous visibility of the HVA cyber hygiene. Similarly, CDM Phase 2 Manage Privilege and Accounts (PRIVMGMT) and Manage Credentials and Authentication (CREDMGMT) capabilities are deployed to better understand the users who have access to the HVA. CDM Phase 3 includes event management capabilities as a requirement. Getting audit logs from HVAs to an event management system will help agency security operations personnel monitor for system and network anomalies. Finally, Phase 4 capabilities, once deployed, will help agencies ensure the data associated with the HVA is protected.

Question 2b. Is it worth prioritizing High-Valued Assets for speedier roll out of CDM capabilities?

Answer. The Department of Homeland Security (DHS) believes that it is worth prioritizing High-Value Assets for deployment of CDM capabilities. While many CDM deployment activities can run in parallel, it will not be possible to deploy all Phase 3 and 4 capabilities to HVAs at one time. As such, prioritization of HVAs will help agencies manage risk and identify where it should be tackled first.

Question 2c. Is it worth considering High-Value Asset data differently in measuring the cybersecurity risk posture of a Federal agency?

Question 2d. Can such a measurement be reflected on the CDM dashboard—both at the agency level and the Federal enterprise dashboard?

Answer. DHS believes that it is worth considering High-Value Asset data differently in measuring the cybersecurity risk posture of a Federal agency. The CDM Program is planning to identify HVAs in the Agency and Federal Dashboards. This identification will enable the Department of Homeland Security and the agencies to assign specific measurements to HVAs that aren't assigned to other non-HVA systems. Additionally, through the implementation of the Agency-Wide Adaptive Risk Enumeration (AWARE) risk measurement algorithm that will be deployed in the summer 2018, DHS will be able to assign different weights to systems and vulnerabilities to draw attention to the most critical issues.

Question 3a. The CDM program is reliant upon system integrators to roll out the solutions of each phase, can you compare the success of each integrator?

Answer. With our partner the General Services Administration (GSA), the Continuous Diagnostics and Mitigation (CDM) Program regularly meets with and monitors the performance of each integrator. Each year, we also complete a Contractor Performance Assessment Report (CPAR) for each integrator. Under our current task orders awarded off the original CDM Blanket Purchase Agreement (BPA), the CPARs are the best way to compare the success of the integrators. Under the new CDM DEFEND acquisition strategy, task orders are being awarded as "cost plus award fee". With these task orders, the program and GSA will be evaluating each integrator semi-annually to measure integrator performance and determine the appropriate award fee level for that half year.

Question 3b. Is there a comparable level of success across the board or do CDM integrators vary in their consistency?

Answer. While the program and GSA have had to address some performance issues with some of the integrators at different points, the integrators are ultimately measured on achieving the objectives of each task order. In that regard, each integrator is making progress toward the successful completion of the task order. With CDM DEFEND, the program will be able to track the performance of each integrator more granularly over the life of each task order.

Question 3c. If so are there any broad lessons learned about managing or choosing integrators?

Answer. One of the key lessons learned throughout the CDM program thus far is the importance of closely monitoring risk for each task order and quickly escalating if the risk increases or becomes an issue. The faster problems can be identified and addressed, the better off all parties will be and the more quickly progress can be made.

Question 4. How has the Information Security Continuous Monitoring (ISCM) strategy been aligned with CDM capabilities and the phased roll-out to ensure an efficient use of taxpayer dollars?

Answer. The Continuous Diagnostics and Mitigation (CDM) Program is the core of the Information Security Continuous Monitoring (ISCM) strategy and the phased roll-out of the program was developed to help reach realization of ISCM. In CDM Phase 3, the program is tackling on-going assessments to help automate the assessment of as many cybersecurity controls as possible with the Phase 1 and 2 tools, as well as those of future phases. The automated controls will then serve as input into the development of on-going authorization, a chief aim of the ISCM strategy.

QUESTIONS FROM CHAIRMAN WILL HURD FOR KEVIN COX

Question 1a. In the Continuous Diagnostics and Mitigation Update dated December 15, 2017 (provided by DHS to the committee), the Phase Two PRIVMGMT Implementation Tracker indicates certain implementation activities are deemed "out of scope for period of performance due to agency not being ready/interested in participating." Are these agencies not interested in implementing CDM privilege management tools in the future?

Answer. Ultimately, all agencies will need to report their PRIVMGMT and CREDMGMT requirements data into the Phase 2 master user record (MUR) that will be a core component of the agency dashboards. For agencies that have or already are deploying PRIVMGMT tools that meet the CDM data requirements, the program did not need to invest further resources in those efforts. In other cases, agencies were focused on other priorities, but intend to participate in the future task orders.

Question 1b. Or, are there plans to move forward with complete implementation that occur after this period of performance (ending 07/11/2018)?

Answer. The CDM DEFEND acquisition strategy was developed so that work for all phases of the CDM Program can occur through each task order. Therefore, the program will be able to work with the agencies and integrators to add new agency requirements when they arise.

Question 1c. Please provide the names of all agencies that have indicated they do not plan to participate in full Phase 2 implementation, meaning complete implementation of PRIVMGMT and CREDMGMT capabilities.

Answer. Because CDM DEFEND will allow the program to work with the agencies and integrators to integrate capabilities as new agencies sign up for CDM or expand their requirements, we do not anticipate at this time that there will be any agencies that do not plan on participating fully in Phase 2 implementations. That being said, the program will inform the committee if any agencies indicate that they will not be participating fully in Phase 2.

QUESTIONS FROM RANKING MEMBER CEDRIC L. RICHMOND FOR KEVIN COX

Question 1. In January, we held a hearing with CDM contractors, who told us that one of the challenges with implementation was the lack of dedicated personnel with the expertise necessary to use CDM technologies and take full advantage of their benefits. Can DHS do anything to address this, perhaps by adding training and labor into contracts for integration services?

Answer. The need for additional training and to help agencies obtain expertise to manage the Continuous Diagnostics and Mitigation (CDM) tools was one of the lessons learned from the original CDM task orders. As a result, the program built mechanisms into the CDM DEFEND acquisition strategy to allow agencies to obtain more subject-matter expert training on the CDM tools. Agencies can also place their own funding on the DEFEND contract if they want to obtain additional training. Additionally, the agencies can use the CDM DEFEND vehicle to obtain additional life-cycle support for their current and future CDM technologies.

Question 2a. The DHS Inspector General recently released a report finding a number of information security vulnerabilities at DHS, including some NPPD systems that were operating without proper authorization. What is the status of DHS's own implementation of CDM?

Answer. The Department of Homeland Security (DHS) Office of the Chief Information Officer continues to make progress in the implementation of Continuous Diagnostics and Mitigation (CDM) throughout the organization.

Question 2b. Has the Department fully deployed Phase 1 technologies?

Answer. DHS is in the process of fully deploying Phase 1 technologies. By the end of the task order period of performance on June 15, 2018, we expect DHS to be at a 95 percent completion level for all networks/components originally scoped for the first DHS Phase 1 contract. The remaining 5 percent included in the original contract scope will be addressed in the follow-on CDM DEFEND contract that was just awarded in May 2018.

Question 2c. Might CDM adoption have been easier or more efficient with a Department-wide cybersecurity strategy in place, as was required under legislation I authored in 2016?

Answer. In November 2013, the Acting Deputy Secretary for DHS issued the "One DHS" Deployment of CDM Capability memo to all component heads, noting the Department's commitment to a leadership role in the Federal Government with regards to cybersecurity. The memo directed DHS components to standardize as much as possible around the common security controls being deployed by CDM and that memo supported CDM deployment throughout the agency. In addition, Secretary Nielsen has signed out the DHS Cybersecurity Strategy, as called for in the 2016 legislation, and places a priority on protecting Federal networks—including DHS's networks.

Question 3a. It looks like DHS has made a lot of progress in getting the so-called "CFO Act agencies" to move forward with CDM adoption, but smaller, non-CFO Act agencies have been more of a challenge. How many of these non-CFO Act agencies is DHS currently working with on CDM?

Answer. The Continuous Diagnostics and Mitigation (CDM) Program currently has memorandums of agreement (MOAs) in place with 56 non-CFO Act agencies. The CDM Shared Service Platform for the non-CFO Act agencies received its authority to operate in March 2018 and the CDM Program is now deploying the CDM Phase 1 and 2 capabilities to these agencies in multiple waves. The CDM Program is currently reaching out to the remaining non-CFO agencies to establish signed MOAs with them to include them as participants in the program.

Question 3b. What tactics can DHS use to grow participation?

Answer. Through our outreach, the program is finding that the non-CFO Act agencies want to participate in the CDM program and get the benefits. When an agency is uncertain, Department leadership is able to engage to help address any concerns and answer any remaining questions.

QUESTIONS FROM RANKING MEMBER ROBIN L. KELLY FOR KEVIN COX

Question 1. What is the time line to roll out Phase 4 data-level protection capabilities as called for in the President's IT Modernization Report and fiscal year 2018/2019 CDM budget requests (see attached)?

Question 2. Have DHS and GSA considered accelerating the adoption of phase 4 capabilities for all .gov agencies?

Answer. Continuous Diagnostics and Mitigation Phase 4 will focus on enhancing data protections for agency high-value assets (HVAs). The program is starting a series of Phase 4 pilots in fiscal year 2018 and is looking to increase Phase 4 efforts

in fiscal year beyond what was originally planned in the program's life-cycle cost estimate.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR KEVIN COX

Question 1a. For your agency, is there any senior cybersecurity leadership positions that remain unfilled?

Question 1b. If so, how has that complicated your ability to move forward with CDM and other information security initiatives?

Answer. The National Protection and Programs Directorate has individuals in the senior cybersecurity leadership positions.

Question 2a. As you know, there is a great deal of diversity among agencies—in terms of their size, structure, and management culture. How is your experience different working with large CFO Act agencies, versus small and micro agencies?

Answer. The largest CFO Act agencies tend to be federated amongst their components and Operational Divisions (OpDivs). This federation introduced challenges in Phase 1. Communication and collaboration were key in overcoming these challenges. With the small- and medium-sized agencies, federation was not as big of an issue. The Continuous Diagnostics and Mitigation (CDM) program still experienced some delays with these agencies due to solution alignment issues within the agency, but the delays tended not to be as prolonged as we saw in the larger agencies.

Question 2b. Are there ways the CDM program could be more responsive to the needs of small- and medium-sized agencies?

Answer. With all sized agencies, communication is a key for success. Through sustained communication with the agencies, the CDM program is able to better understand the agency needs and unique requirements. The program can then work with the integrator to shape the CDM solution appropriately for each agency. Good, sustained communication takes work, but offers a good pay-off.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR KEVIN COX

Question 1. NPPD's Congressional Justification for its fiscal year 2019 budget request does not describe any efforts by CDM to provide asset management, identity management, network monitoring, or data protection capabilities for cloud-based services. Cloud security is not mentioned in the CDM Technical Capabilities documents published by GSA (Volumes One and Two). On March 20, you testified that your intention with CDM Phase 3 was to provide agencies with "visibility of their data and their networks . . . wherever that data is, whether it's out in the cloud, whether it's on a mobile device, wherever it's stored or used." What tools and services will CDM provide to Federal agencies to secure their cloud services?

Answer. The Continuous Diagnostics and Mitigation (CDM) Technical Capabilities documents are updated at least annually. Cloud, mobile, and many of the other Phase 3 efforts will be addressed in the next update. As for the CDM approach for cloud, the program is working to develop the appropriate approach for continuous monitoring in the cloud. Given the differences between on-premise and cloud architectures, the CDM program will not be able to approach cloud environments the same way we did for on-premise networks (e.g., we won't be deploying individual sensors on each Virtual Machine (VM) in the cloud, as these VMs can change frequently). Rather, we are looking to achieve continuous monitoring in the cloud through multiple mechanisms that are in the process of being developed. These may include a network security stack in front of the cloud environment, data interfaces to the security controls provided by the cloud service providers (CSPs), and visibility into data from other security capabilities provided either by the CSP or a third-party entity.

Question 2. As we know from the critical infrastructure community, cybersecurity must extend beyond desktop computers. Within DHS, for example, Border Patrol, TSA, and FEMA agents employ diverse sensors and communications systems that don't run on Windows. What tools and services will CDM provide to Federal agencies to help protect mobile, operational, or other networked devices with uncommon operating systems?

Answer. Many of the Continuous Diagnostics and Mitigation (CDM) Phase 1 tools provide continuous visibility for many versions of Unix/Linux and MacOS. However, not all operating systems are covered by all tools. Where we have identified gaps, we plan on working with the CDM DEFEND integrators to identify the best technology to help fill those gaps. This will be an on-going effort, particularly as more Internet of Things devices come on-line. As for mobile, we will interface with each agency's Enterprise Mobility Management (EMM) system to gain visibility into the devices and mobile apps in use in the environment. If an agency does not have an

EMM, we will work with the agency and the integrator to identify the optimal EMM solution for the agency.

Question 3. The DEFEND contract moved CDM away from implementing identical tools and toward helping agencies procure a variety of tools and services from an approved list. This flexibility will likely result in unique cybersecurity implementations, making it more difficult to share and reuse collected data, and increasing the cost of integrating new tools in the future. What guidance is DHS providing to agencies to encourage reuse, sharing, and interoperability of cybersecurity data and tools?

Answer. The key to making the additional flexibility work is to use technologies from vendors that participate in and use common data interface standards. The Continuous Diagnostics and Mitigation (CDM) program is building these into our requirements. As long as a product meets these standards, gaining access to the data that fulfills the CDM requirements is a pretty direct process. We know from experience that this can work based on the many different CDM technologies in use today. Based on our experience so far, we expect most agencies will settle on a single tool throughout their agency for each respective CDM capability. The flexibility gains a lot of value when agencies are able to use existing tools already in place to meet future CDM data requirements, as long as we can establish an interface to the data. The benefits include more willing agency participation, potential cost savings, and fewer scenarios where agencies must remove existing tools and replace with CDM tools.

Question 4. What metrics are you collecting to demonstrate that CDM has successfully improved cybersecurity in the adopting agencies?

Answer. The Continuous Diagnostics and Mitigation (CDM) Program has developed a series of metrics demonstrating cost savings compared to General Services Administration IT Schedule 70, significant asset and user discovery improvements, and millions of assets now having near real-time cybersecurity sensors in place. We are continuing to build on these to show how the agencies are starting to use the CDM tools to reduce their attack surface and improve their overall cyber hygiene. During the summer of 2018, the CDM program is also introducing the Agency-Wide Adaptive Risk Enumeration (AWARE) algorithm that will allow agencies to compare their security posture over time against their original baseline. It will also give Federal leadership a tool to measure agency cybersecurity performance. The AWARE algorithm will be implemented by late fiscal year 2018 and will be operationalized through fiscal year 2019.

Question 5. CDM represents a large investment of dollars and time. I would like to understand how we will know that investment has been successful, in terms of improved security across the dot-gov domain. How extensive are the cybersecurity staff and skills shortfalls in your program, and how are they affecting your ability to execute the program?

Answer. The key to showing the success of the investment is through metrics like the Agency-Wide Adaptive Risk Enumeration (AWARE) algorithm. By baselining agencies at the start, it gives us a way to measure improvement over time. The Continuous Diagnostics and Mitigation program can already show that success today through metrics like the significant asset discovery improvements and the total number of assets reporting to the Federal Dashboard that have security sensors in place that can report the near real-time vulnerability and configuration state of each asset. The AWARE algorithm will pull all of the various measures into a singular score that will be standardized and allow for comparisons between agencies.

In regards to staff in the CDM Program, we have a skilled, dedicated team of 40 people and are in the process of hiring and performing security clearances on an additional 14. Through recent staffing planning, the estimated personnel needs are known for the work associated with Phases 3 and 4 and included in the life-cycle cost estimates of the program used to inform future year budget requests.