AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ASSESSING THE STATE OF FEDERAL CYBERSECURITY RISK DETERMINATION

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 25, 2018

Serial No. 115–73

Printed for the use of the Committee on Homeland Security



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

U.S. GOVERNMENT PUBLISHING OFFICE

34–445 PDF WASHINGTON : 2019

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
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
DEBBIE LESKO, Arizona

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, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

JOHN RATCLIFFE, Texas, *Chairman*

JOHN KATKO, New York
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
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*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable John Ratcliffe, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:
Oral Statement 1
Prepared Statement 3
The Honorable Cedric L. Richmond, a Representative in Congress From the State of Louisiana, and Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection:
Oral Statement 4
Prepared Statement 5
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Prepared Statement 6

WITNESSES

Mr. Ken Durbin, Senior Strategist, Global Government Affairs, Symantec:
Oral Statement 8
Prepared Statement 9
Ms. Summer Fowler, Technical Director, Cybersecurity Risk and Resilience, Software Engineering Institute, CERT, Carnegie Mellon University:
Oral Statement 13
Prepared Statement 14
Mr. Ari Schwartz, Managing Director of Cybersecurity Services, Cybersecurity Risk Management Group, Venable LLP, Testifying on Behalf of the Cybersecurity Coalition and Center for Cybersecurity Policy and Law:
Oral Statement 18
Prepared Statement 19

APPENDIX

Questions From Honorable James R. Langevin for Summer Fowler 33
Questions From Honorable James R. Langevin for Ari Schwartz 34

ASSESSING THE STATE OF FEDERAL CYBERSECURITY RISK DETERMINATION

Wednesday, July 25, 2018

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

The subcommittee met, pursuant to notice, at 10:38 a.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe (Chairman of the subcommittee) presiding.

Present: Representatives Ratcliffe, Bacon, Donovan, Katko, Richmond, and Langevin.

Mr. RATCLIFFE. Good morning. The Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection will come to order.

The subcommittee is meeting this morning to receive testimony regarding how the Federal Government understands and manages enterprise-wide cybersecurity risks. I now recognize myself for an opening statement.

As we convene today, this subcommittee is concerned that the Federal Government is not yet equipped to determine how threat actors seek to gain access to our private information. This challenge is one of the reasons I introduced, and yesterday the full committee passed, the Advancing Cybersecurity Diagnostics and Mitigation Act. H.R. 6443 will codify and provide direction to DHS regarding the CDM program. This was a bipartisan effort and I thank the Ranking Member, Mr. Richmond, as well as Mr. Katko, Mr. Donovan, Mr. Fitzpatrick, and Mr. Langevin, for working with me on this important issue because there is an evident lack of strategy in mitigating risk across our Federal agencies.

Cyber work force gaps and legacy IT systems are vulnerabilities in the Federal Government's cybersecurity posture but the efficacy of our basic cybersecurity practices remain common liabilities. To this end the Office of Management and Budget and Department of Homeland Security released a report earlier this year entitled Federal Cybersecurity Risk Determination Report Action Plan. This report spoke to many of the challenges faced in securing enterprise-wide Federal Government IT systems.

Perhaps not surprisingly OMB and DHS determined that 74 percent of Government agencies have cybersecurity programs that are either at risk or at high risk. The risk assessments performed by these agencies showed that a lack of threat information results in ineffective allocations of limited cyber resources. This overall situa-

tion creates enterprise-wide gaps in our network visibility, IT tool, and capability standardization, and common operating procedures, all of which negatively impact Federal cybersecurity.

Given the significant and ever-increasing danger of threats and the absence of good data inventory, risk management must be fully integrated into every aspect of an organization. Leaders of Federal agencies at all organizational levels must understand the responsibilities and they must be accountable for protecting organizational assets and managing security and privacy risks.

The OMB and DHS report identified four main actions that are necessary to address cybersecurity risks across the Federal enterprise. First, Federal agencies must increase their cybersecurity threat awareness. This seems like a too obvious of a recommendation but often those charged with defending agency networks lack timely information regarding the tactics, techniques, and procedures that our adversaries are using to exploit Government information systems.

Second, OMB urged agencies to standardize IT and cybersecurity capabilities to control costs and to improve asset management. Generally speaking agencies do not have standardized cybersecurity processes, which ultimately impacts their ability to efficiently and effectively combat cyber threats.

The Continuous Diagnostics and Mitigation program or CDM will accelerate both IT management efforts and cybersecurity improvements across the Federal Government. In fact, my bill, the Advancing Cybersecurity Diagnostics and Mitigation Act will require the program to evolve thereby ensuring that agency CIOs and DHS have the visibility necessary, not only to combat threats, but also to target modernization resources and efforts where they are most needed.

The third recommended action is that agencies must consolidate their security operation centers to improve incident detection and response capabilities. OMB found that only 27 percent of agencies can detect and investigate attempts to access large volumes of data. This troubling statistic should cause us all to pause.

While the report identifies that Federal agencies currently lack network visibility, the DHS's CDM program can assist with this issue by providing insight into what is occurring on networks—after all, you cannot defend what you cannot see.

Finally, OMB recommended that agencies increase accountability through improved governance processes, indeed both the Federal Information Security Management Act and President Trump's Executive Order on Strengthening the Cybersecurity and Federal Networks and Critical Infrastructure already identify the agency head as the official ultimately responsible for each agency's cybersecurity.

Of course, agency heads often delegate cyber risk management responsibilities to the chief information officer and chief information security officer but agency leadership should increase its oversight of and its engagement in their agency's cybersecurity ecosystem.

Ultimately a collaborative approach to mitigating cyber threats is meant to prioritize meeting the needs of DHS's partners and is consistent with the growing recognition among Government, academic,

and corporate leaders, that cybersecurity is increasingly interdependent across sectors and must be a core aspect of risk management strategies.

We are in an era that requires flexibility, resiliency, and discipline. I look forward to a candid conversation with our witnesses today about ensuring our Federal networks can embody these goals. Your thoughts and opinions are important as we oversee the state of Federal Government cybersecurity risks.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

JULY 25, 2018

This subcommittee is concerned that the Federal Government is not equipped to determine how threat actors seek to gain access to private information. There is an evident lack of strategy in mitigating risk across Federal agencies. Cyber workforce gaps and legacy IT systems are vulnerabilities in the Federal Government's cybersecurity posture, but the efficacy of our basic cybersecurity practices are common liabilities.

To this end, the Office of Management and Budget and Department of Homeland Security released a report earlier this year entitled "Federal Cybersecurity Risk Determination Report and Action Plan." This report spoke to many of the challenges faced in securing enterprise-wide Federal Government IT systems.

Perhaps not surprisingly, OMB and DHS determined that 74 percent of Government agencies have cybersecurity programs that are either at-risk or high-risk. The risk assessments performed by these agencies showed that a lack of threat information results in ineffective allocations of limited cyber resources. This overall situation creates enterprise-wide gaps in network visibility, IT tool and capability standardization, and common operating procedures, all of which negatively impact Federal cybersecurity.

Given the significant and ever-increasing danger of threats and the absence of good data inventory, risk management must be fully integrated into every aspect of an organization. Leaders of Federal agencies at all organizational levels must understand their responsibilities and must be accountable for protecting organizational assets and managing security and privacy risks.

The OMB and DHS report identified four main actions that are necessary to address cybersecurity risks across the Federal enterprise. First, Federal agencies must increase their cybersecurity threat awareness. This seems like too obvious of a recommendation, but often, those charged with defending agency networks lack timely information regarding the tactics, techniques, and procedures that adversaries use to exploit Government information systems.

Second, OMB urged agencies to standardize IT and cybersecurity capabilities to control costs and improve asset management. Generally speaking, agencies do not have standardized cybersecurity processes, which ultimately impacts their ability to efficiently and effectively combat threats. The Continuous Diagnostics and Mitigation program, or CDM, will accelerate both IT management efforts and cybersecurity issues across the Federal Government. In fact, a bill that I introduced last week H.R. 6443, the Advancing Cybersecurity Diagnostics and Mitigation Act, will require the program to evolve to ensure agency CIO's and DHS have the visibility necessary not only to combat threats, but also to target modernization resources and efforts where they are most needed.

Third, agencies must consolidate their security operations centers to improve incident detection and response capabilities. OMB found that only 27 percent of agencies can detect and investigate attempts to access large volumes of data. This troubling statistic should cause all of us to pause. While the report identifies that Federal agencies currently network visibility, DHS's CDM program can assist with this issue by providing insights into what is occurring on networks. After all you can't defend what you can't see.

And finally, OMB recommended that agencies increase accountability through improved governance processes. Indeed, both the Federal Information Security Management Act and President Trump's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure already identify the agency head as the official ultimately responsible for each agency's cybersecurity. Of course, agency heads often delegate cyber risk management responsibilities to the chief in-

formation officer and chief information security officer, but agency leadership should increase its oversight of, and engagement in, their agency's cybersecurity ecosystem.

Ultimately, a collaborative approach to mitigating cyber threats is meant to prioritize meeting the needs of DHS partners, and is consistent with the growing recognition among Government, academic, and corporate leaders that cybersecurity is increasingly interdependent across sectors and must be a core aspect of risk management strategies.

We are in an era that requires flexibility, resiliency, and discipline, I look forward to a candid conversation with our witnesses about ensuring Federal networks can embody these goals. I look forward to hearing from our witnesses. Your thoughts and opinions are important as we oversee the state of Federal Government cybersecurity risks.

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

Mr. RICHMOND. Good morning.

I want to thank Chairman Ratcliffe for holding today's hearing on the Federal Cybersecurity Risk Determination Report and Action Plan.

It is no secret that Federal networks are an attractive target to our adversaries and cyber criminals alike. Thales eSecurity 2018 Data Threat Report found Federal agencies experienced more data breaches than any other sector.

State actors such as Russia, China, Iran, and North Korea have become more sophisticated, more emboldened and more brazen and the data stored on our networks about American citizens, our National security plans, and our economy, is important to them.

We have authorized and funded programs to defend our Federal networks and this subcommittee has performed rigorous oversight over many of them, this Congress. I am familiar with the challenges related to implementation of the Department of Homeland Security's Continuous Diagnostics and Mitigation program, CDM, as well as cyber threat information sharing so I was not terribly surprised by some of the Federal cybersecurity risk determination reports general findings.

But the devil is in the details. I could have told you for example that the collective ability of our Federal agencies to understand what is happening on their networks isn't what it should be but I did not realize that fewer than half of the 96 agencies surveyed can detect encrypted ex-filtration of information at target levels or that only 27 percent can detect and investigate attempts to access large volumes of data.

I knew that resource challenges have stunted the maturation of programs designed to protect Federal networks but I was troubled to learn that agencies are not equipped to make strategic investment decisions with money Congress provides.

While I could have assumed that agencies could improve their Cyber Incident Response procedures or how cyber risks are communicated, I could not have predicted that just over half of the agencies surveyed had validated Cyber Incident Response roles in the past year and only 59 percent of agencies have a mechanism to issue enterprise-wide cyber threat alerts. We have to do better than this.

The Federal Cybersecurity Risk Determination Report identified important actions the Federal Government should undertake to resolve existing capability gaps. Many of the proposed solutions le-

verage CDM tools, some of which have yet to be fully implemented or may not be deployed anytime soon.

Yesterday, this committee approved legislation Chairman Ratcliffe introduced, and which I co-sponsored, to make the CDM program more robust, more accountable. I would be interested in hearing from our witnesses about how the Federal Government can optimize the potential of CDM and improve its implementation.

Additionally, I would be interested to know if the witnesses disagree with any of the action items identified in the risk determination report or if they are critical or issues critical to risk management that the report failed to address.

Finally, I will be interested in hearing the witnesses' thoughts about the importance of leadership from the White House when it comes to improving the cybersecurity of our Federal networks.

Before I close I want to point out on a separate subject that we are heading into August recess without making any progress toward reauthorization of the Chemical Facility Anti-Terrorism Standards, known as the CFATS program.

Ranking Member Thompson and I have repeatedly asked the Majority to hold oversight hearings with the Department and begin work on negotiating and forming CFATS' reauthorization legislation. Neither has happened and I am concerned that we may not have enough legislative days left to get reauthorization past the finish line. I hope the majority will make CFATS a priority when we return from the August recess so we can avoid a temporary extension.

With that I thank the witnesses for being here today. I look forward to their testimony.

I yield back the balance of my time.

[The prepared statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC RICHMOND

JULY 25, 2018

Good morning. I would like to thank Chairman Ratcliffe for holding today's hearing on the Federal Cybersecurity Risk Determination Report and Action Plan.

It is no secret that Federal networks are an attractive target to our adversaries and cyber criminals alike.

Thales e-Security's 2018 Data Threat Report found Federal agencies experience more data breaches than any other sector.

State actors—such as Russia, China, Iran, and North Korea—have become more sophisticated, more emboldened, and more brazen.

And the data stored on our networks—about American citizens, our National security plans, and our economy—is important to them.

We have authorized and funded programs to defend our Federal networks, and this subcommittee has performed rigorous oversight over many of them this Congress.

I am familiar with the challenges related to implementation of the Department of Homeland Security's Continuous Diagnostic and Mitigation Program (CDM) as well as cyber threat information sharing.

So I wasn't terribly surprised by some of the Federal Cybersecurity Risk Determination Report's general findings.

But the devil is in the details.

I could have told you, for example, that the collective ability of our Federal agencies to understand what is happening on their networks isn't what it should be.

But I didn't realize that fewer than half of the 96 agencies surveyed can detect encrypted exfiltration of information at target levels, or that only 27 percent can detect and investigate attempts to access large volumes of data.

I knew that resource challenges have stunted the maturation of programs designed to protect Federal networks, but I was troubled to learn that agencies are

not equipped to make strategic investment decisions with the money Congress provides.

And, while I could have assumed that agencies could improve their cyber incident response procedures or how cyber risks are communicated, I could not have predicted that just over half of the agencies surveyed had validated cyber incident response roles in the past year and only 59 percent of agencies have a mechanism to issue enterprise-wide cyber threat alerts.

We have to do better than this.

The Federal Cybersecurity Risk Determination Report identified important actions the Federal Government should undertake to resolve existing capability gaps.

Many of the proposed solutions leverage CDM tools, some of which have yet to be fully implemented or may not be deployed any time soon.

Yesterday, this committee approved legislation Chairman Ratcliffe introduced, and which I cosponsored, to make the CDM program more robust and more accountable.

I will be interested to hear from our witnesses about how the Federal Government can optimize the potential of CDM and improve its implementation.

Additionally, I would be interested to know if the witnesses disagree with any of the action items identified by the Risk Determination Report or if there are issues critical to risk management that the report failed to address.

Finally, I will be interested in hearing the witnesses' thoughts about the importance of leadership from the White House when it comes to improving the cybersecurity of our Federal networks.

Before I close, I want to point out that we are heading into August recess without making any progress toward reauthorization of the Chemical Facility Anti-Terrorism Standards (CFATS) program.

Ranking Member Thompson and I have repeatedly asked the Majority to hold oversight hearings with the Department and begin work on negotiating informed CFATS reauthorization legislation.

Neither has happened, and I am concerned that we may not have enough legislative days left to get reauthorization past the finish line.

I hope the Majority will make CFATS a priority when we return from August recess so we can avoid a temporary extension.

With that, I thank the witnesses for being here today, and I look forward to their testimony.

I yield back the balance of my time.

Mr. RATCLIFFE. I thank the gentleman.

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

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 25, 2018

Good morning. I want to thank Chairman Ratcliffe and Ranking Member Richmond for holding today's hearing on the "State of Federal Cybersecurity Risk Determination".

At the outset, I would like to echo Ranking Member Richmond's disappointment that we are heading into August recess without making any meaningful progress on reauthorizing the Chemical Facility Anti-Terrorism Standards Program (CFATS), which expires in less than 6 months.

As far as I know, the CFATS program has bipartisan support on this committee. It is also popular with the regulated community, and, most importantly, makes our communities safer.

Given the limited number of legislative days left, I hope this committee acts quickly when we return in September to fulfill our obligations as authorizers and put CFATS on the track to reauthorization.

Turning to the subject of today's hearing—although I am pleased that OMB and DHS have undertaken a review of the risk determination and acceptance choices across the Federal Government, I am troubled that many of our cybersecurity capabilities are not as mature as they ought to be.

When I joined the Select Committee on Homeland Security in 2003, every expert I heard from told me that the Federal Government was 10 years behind where it should in with respect to cybersecurity.

Despite the investments we have made since then, it seems we are in the same boat—10 years behind where we need to be.

Federal agencies still struggle to access timely, actionable threat information and share it enterprise-wide.

Agencies still do not have full visibility of what is happening on their networks or who has access to different pieces of information.

And we still have not figured out how to strategically allocate funding to address risk.

Despite the devastating data breaches like the 2015 Office of Personnel Management heist of the personal information of 22.1 million people, non-defense agencies spent less than $51 million encrypting data rest in fiscal year 2017.

Meanwhile, of the $80 billion we spend annually on IT systems across the Federal Government, 80 percent is spent maintaining legacy systems that are more vulnerable and less secure.

We need to start putting our money where the risk is.

This is not the first time we have heard these recommendations.

So, there is one thing I would like to know from our witnesses today: How can the Federal Government finally jump the 10-year gap between where we are and where we should be?

I know it will take technology. I know it will take money. And, importantly, I know it will take leadership.

I am concerned that the White House has limited its ability to lead as effectively as it could in this space by eliminating the Cybersecurity Coordinator position and dragging out the appointment of the Federal CIO and CIOs and large agencies.

Nevertheless, as Members of Congress, we will continue our rigorous oversight to hold the administration accountable for the action items outlined in the *Federal Cybersecurity Risk Determination Report and Action Plan.*

With that, I look forward to hearing from our witnesses, and I yield back the balance of my time.

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

Mr. Ken Durbin is a senior strategist of global government affairs for Symantec. Mr. Durbin has been providing compliance and risk management solutions to the public sector for over 25 years and has authored multiple articles on CRM issues. Thank you for being here this morning.

Ms. Summer Fowler is the technical director for the cybersecurity, risk, and resilience in the Software Engineering Institute at Carnegie Mellon. In this role Ms. Fowler is responsible for executing the strategic plan for a research portfolio focused on improving the security and resilience of organizational assets. Ms. Fowler, thank you for being here to provide your insights today.

Finally, Mr. Ari Schwartz is the managing director of cybersecurity services in the risk management group of Venable. Mr. Schwartz is testifying today on behalf of the Cybersecurity Coalition and Center for Cybersecurity Policy and Law.

Prior to his time at Venable, Mr. Schwartz served on the National Security Council as a special assistant to the President, and senior director for cybersecurity. Thank you for being here today Mr. Schwartz.

I would now ask the witnesses to stand and raise your right hand, so I can swear you in to testify.

[Witnesses sworn.]

Let the record reflect that each of the witnesses has been so sworn. You may be seated.

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

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

STATEMENT OF KEN DURBIN, SENIOR STRATEGIST, GLOBAL GOVERNMENT AFFAIRS, SYMANTEC

Mr. DURBIN. Chairman Ratcliffe, Ranking Member Richmond, thank you for the opportunity to testify.

I would like to start by setting the stage with regards to the current threat landscape. Attackers continue to evolve; to avoid detection, attackers are employing what we call living-off-the-land—using operating system features or legitimate network administration tools to compromise victim's networks.

Using good programs to do bad things is difficult to detect because it is disguised as normal operations. We recently discovered one such attack that had compromised satellite operators, telecommunications companies, and a defense contractor.

We identified the attack using an advanced hunting tool we call "Targeted Attack Analytics" which crawls through massive datasets looking for minute indicators of malicious activity.

Cryptojacking is another common attack. We have seen the rise of a new category of web-based coin-miner attacks that use an individual's browser to hijack their computer's processing power to mine cryptocurrency. Detections of coin-miners on endpoint computers increased by 8,500 percent in 2017.

We saw an uptick in supply chain attacks where attackers hijacked software updates to gain entry to well-guarded networks. The Petya outbreak was the most notable example of a supply chain attack. Attackers used accounting software as the point of entry.

Now turning to the Federal Cybersecurity Risk Determination Report and Action Plan, the report is a tough but fair assessment of the current state of the Executive branch's cybersecurity posture and it looks to build on existing security frameworks to make improvements.

I want to take a moment to commend OMB for recognizing the value of the NIST Cybersecurity Framework or CSF as a tool to improve the current state of the Executive branch's risk management efforts.

Typically, an agency collects data from over 200 FISMA controls, across 10 control families, to evaluate cybersecurity readiness. That same data can be consolidated into the 5 CSF functions for a clearer view into their cyber readiness. The report made several recommendations.

In the first the report notes that 38 percent of Federal cyber incidents did not have an identified attack vector and recommends implementing the Cyber Threat Framework or CTF to help categorize cybersecurity risks. However, it is not clear how categorizing attacks would have helped protect against the cyber events that compromised information and systems.

To reduce the number of identified attacks, I recommend that along with implementing the CTF, OMB put a strong emphasis on cybersecurity solutions that automate the detection and remediation of cyber events through communication between strategic control points, hunting for indicators that are compromised.

I commend OMB's efforts to develop a risk-based budget process to direct IT purchases to reduce identified risk. Another way to reduce identified risk would be to require agencies to add rec-

ommendations contained in IG FISMA audits as line items in their budget requests to ensure they receive adequate prioritization.

The report also recommends standardizing IT and cybersecurity capabilities. This can be achieved through the Continuous Diagnostics and Mitigation or CDM program. CDM achieves the same goals by focusing on standardized capabilities rather than a standardized vendor. However, the CDM program needs to be accelerated: 5 years after CDM was launched, phase 1 to 4 has still not been fully deployed.

The third recommendation is to consolidate agency security operation centers to improve overall incident detection and response. While this is part of the solution, detecting the ex-filtration of data requires more than consolidation, which brings me to the fourth recommendation, accountability.

I want to focus on the data-level protection's aspect of this recommendation. Far too often we see the Government equate data-level protection with the encryption of data. While encryption is important, the Government's focus needs to be expanded to include prevention, specifically data loss prevention or DLP. DLP can discover and categorize sensitive data and can enforce policies about what can be done with that data. DLP can automatically encrypt data before it is transmitted even if the end-user forgot to encrypt it themselves.

I recommend that DHS advance the data protection phase of CDM which would have the added benefit of protecting the high-value assets identified by agencies during the 2015 Cyber Sprint.

I hope these observations build on OMB's recommendations and maximize their ability to improve our Government cybersecurity posture.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Durbin follows:]

PREPARED STATEMENT OF KEN DURBIN

JULY 25, 2018

Chairman Ratcliffe, Ranking Member Richmond, my name is Ken Durbin, CISSP, and I am a senior strategist for Symantec Global Government Affairs and Cybersecurity. I have been providing solutions to the public sector for over 30 years. My focus on compliance and risk management (CRM) and the critical infrastructure sector has allowed me to gain insights into the challenge of balancing compliance with the implementation of cybersecurity solutions. Additionally, I focus on the standards, mandates, and best practices from NIST, OMB, DHS, SANS, etc. and their application to CRM. I spend a significant amount of my time on the NIST Cybersecurity Framework (CSF)[1], the DHS CDM Program and the emerging EU Global Data Protection Regulation (GDPR.)

Symantec Corporation is the world's leading cybersecurity company and has the largest civilian threat collection network in the world. Our Global Intelligence Network™ tracks over 700,000 global adversaries, records events from 126.5 million attack sensors world-wide, and monitors threat activities in over 157 countries and territories. Additionally, we process more than 2 billion emails and over 2.4 billion web requests each day. We maintain 9 Security Response Centers and 6 Security Operations Centers around the globe, and all of these resources combined give our analysts a unique view of the entire cyber threat landscape. On our consumer side, we combined Norton Security with LifeLock's Identity and Fraud Protection to deliver a comprehensive cyber defense solution to a growing consumer base of nearly 4.5 million people.

[1] NIST Cybersecurity Framework (CSF): Provides guidance to private companies on how best to prevent, detect, and respond to cyber attacks.

In my testimony I will provide:
- an overview of the current threat landscape, including highlights of our 2018 Internet Security Threat Report (ISTR),[2]
- an assessment of the Federal Cybersecurity Risk Determination Report and Action Plan that was released in May,
- high-level recommendations on addressing some of challenges highlighted in the report.

THE THREAT LANDSCAPE

From the recent Thrip attack on satellite and telecommunications systems to the spread of WannaCry and Petya/NotPetya, to the rapid growth in coinminers, the past year has provided us with many reminders that digital security threats can come from new and unexpected sources. With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so. Symantec's annual ISTR provides a comprehensive view of the threat landscape, including insights into global threat activity, cyber criminal trends, and motivations for attackers. Below are some key highlights from this year's report and our recent work.

Attackers are Evolving

Last month, we issued a report about a previously unknown attack group known as Thrip.[3] Thrip is a sophisticated attacker that used a technique we call "living off the land"—using operating system features or legitimate network administration tools to compromise victims' networks. Simply put, they use good programs to do bad things. These types of attacks are difficult to detect because malicious activity is disguised as normal system operations. This continued a trend we reported on in the ISTR, that attackers are relying less on malware and zero-day vulnerabilities. Instead, they are looking for new attack vectors that make less "noise" and can be hard for some defenders to detect.

When we discovered Thrip, they had already compromised satellite operators, telecommunications companies, and a defense contractor. We identified this malicious activity using an advanced hunting tool we call Targeted Attack Analytics, which crawls through massive data sets looking for minute indicators of malicious activity. When we find something—like Thrip—we update our protections to stop it in the future. Thrip was not the first living off the land attack, and it will not be the last, and defenders must evolve to stay ahead of the next attack.

Cryptojacking

During the past year, an astronomical rise in cryptocurrency values triggered a cryptojacking gold rush with cyber criminals attempting to cash in on a volatile market. This gave rise to a new category of malware called "coinminers" that attach to an individual's browser and utilizes their computers processing power to mine cryptocurrency. Detections of coinminers on endpoint computers increased by 8,500 percent in 2017. With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are harnessing stolen processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency. Coinminers can slow devices, overheat batteries, and in some cases, render devices unusable. For enterprise organizations, coinminers can put corporate networks at risk of shutdown and inflate cloud CPU usage, adding cost. Macs are not immune either, with Symantec detecting an 80 percent increase in coinmining attacks against Mac OS. By leveraging browser-based attacks, criminals do not need to download malware to a victim's Mac or PC to carry out cyber attacks.

IoT

IoT devices continue to be ripe targets for exploitation. Symantec found a 600 percent increase in overall IoT attacks in 2017, which means that cyber criminals could exploit the connected nature of these devices to mine en masse.

Targeted Attack Groups

The number of targeted attack groups is on the rise with Symantec now tracking 140 organized groups. Last year, 71 percent of all targeted attacks started with spear phishing—the oldest trick in the book—to infect their victims. As targeted at-

---

[2] *https://www.symantec.com/security-center/threat-report.*

[3] *https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets?om__ext__cid=biz__social__NAM__twitter__Asset%2BType%2B%2B-%2BBlog,Campaign%2B-%2BThreat%2BAlert.*

tack groups continue to leverage tried and true tactics to infiltrate organizations, the use of zero-day threats is falling out of favor. Only 27 percent of targeted attack groups have been known to use zero-day vulnerabilities at any point in the past. The security industry has long discussed what type of destruction might be possible with cyber attacks. This conversation has now moved beyond the theoretical, with 1 in 10 targeted attack groups using malware designed to disrupt.

Supply Chain Attacks

Symantec identified a 200 percent increase in attackers injecting malware implants into the software supply chain in 2017. That's equivalent to 1 attack every month as compared to 4 attacks the previous year. Hijacking software updates provides attackers with an entry point for compromising well-guarded networks. The Petya outbreak was the most notable example of a supply chain attack. After using Ukrainian accounting software as the point of entry, Petya used a variety of methods to spread laterally across corporate networks to deploy their malicious payload.

Ransomware for Profit

In 2016, the profitability of ransomware led to a crowded market. In 2017, the market made a correction, lowering the average ransom cost to $522 and signaling that ransomware has become a commodity. Many cyber criminals may have shifted their focus to coin mining as an alternative to cashing in while cryptocurrency values are high. Additionally, while the number of ransomware families decreased, the number of ransomware variants increased by 46 percent, indicating that criminal groups are innovating less but are still very productive.

ASSESSMENT OF THE FEDERAL CYBERSECURITY RISK DETERMINATION REPORT AND ACTION PLAN

The Office of Management and Budget (OMB), in response to Presidential Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* produced a report that provides a tough but fair assessment of the current state of the Executive branch's Cybersecurity Posture. The EO and the report builds upon the efforts of previous administrations and works within existing frameworks, including FISMA,[4] FITARA,[5] CDM,[6] and CSF. While none of these are perfect, OMB sees their value and seeks to improve them. The EO held OMB to a tight time line in which to produce the report and OMB held agencies to a similarly aggressive time line. This alone sent a strong message, both about the seriousness of the situation and about the administration's commitment to improving the Executive branch's cybersecurity posture.

As a threshold matter, I would like to commend the administration and OMB for recognizing the value of the CSF as a tool to improve the current state of the Executive branch's risk management efforts. The CSF's power is its ability to take a complex set of cybersecurity data and present them in a clear, logical, and simplified way such that one does not need to be a cyber expert to gain valuable insight and make important decisions. For example: An agency now needs to collect data from over 200 FISMA controls across 10 control families to evaluate cybersecurity readiness. That same data can be consolidated into the 5 CSF functions (identify, protect, detect, respond, and recover) for a clearer view into their cyber readiness.

Recommendation No. 1: Increase Cybersecurity Threat Awareness

To highlight the need for increasing cybersecurity threat awareness, the report points out that "38 percent of Federal cyber incidents did not have an identified attack vector." This equates to 11,802 cyber incidents that "led to the compromise of information or system functionality in fiscal year 2016." To improve this situation the report recommends implementing the Cyber Threat Framework (CTF) with the idea that it will help prioritize and manage cybersecurity risks. The CTF was developed to enable consistent characterization and categorization of cyber threat events; in other words, to provide a common lexicon to describe and understand threats. This, of course is a worthwhile pursuit, but it is not clear how the CTF would have helped protect against the 11,802 cyber events that compromised information and systems.

---

[4] Federal Information Security Management Act: Requires Government agencies to implement security systems to protect information and information systems.

[5] Federal Information Technology Acquisition Reform Act: Changed the way the Federal Government buys and manages its computer technology.

[6] Continuous Diagnostics and Mitigation: Four-phase program that monitors what is on a network, who is on a network, what is happening on a network, and how data is protected for Federal agencies.

I recommend that, along with implementing the CTF, OMB put a strong emphasis on cybersecurity solutions that can automate the detection and remediation of cyber events. Automated cybersecurity solutions that can communicate between strategic control points hunting for indicators of compromise (IoCs) will help to reduce the number of unidentified attacks, and reduce the burden caused by the shortage of qualified cyber professionals.

I applaud OMB's efforts to develop a risk-based budgeting process to help direct IT purchases toward products, solutions, and services that will have a direct impact on reducing identified risk. OMB may want to consider taking this effort one step further to address one long-standing issue around agency IG Report recommendations. IG Reports regularly contain risk-based recommendations that are carryovers from previous year's reports, and often they remain unresolved due to budget or staffing issues. Adding IG recommendations as line items in an agency's budget request could be a way to ensure the recommendations receive adequate prioritization. Additionally, DHS has modified the CDM program to allow agencies to submit Requests for Service (RFS) to fulfill specific needs. Known as CDM DEFEND, this may be another vehicle to address risk-based procurement.

Recommendation No. 2: Standardize IT and Cybersecurity Capabilities

This recommendation harkens back to the massive GSA "desktop" contracts of the 1980's and 1990's. For the most part those contracts mandated a standardized PC platform with specific software preinstalled. (The original contract required a Zenith 286 with DOS, Harvard Graphics, Lotus123, and WordStar.) This did have some of the same advantages spelled out in the report, including consistent software versions, ease of patching, known configurations, and simplified troubleshooting. The downside was that even if a competitor of Zenith had a better PC it was next to impossible to justify not using the desktop contract.

I believe the Continuous Diagnostics and Mitigation (CDM) concept achieves the goals set forth in this recommendation by focusing on standardized capabilities rather than a standardized vendor. However, in order to be effective in meeting this goal, the CDM Program will need move faster—5 years after CDM was launched Phase 1 has still not been fully deployed. DHS has taken steps to accelerate the program, launching CDM DEFEND, which utilizes the GSA Alliant Contract and extends the period of performance of awarded Task Orders.

Recommendation No. 3: Consolidate Agency SOCs

Redundant Security Operation Centers (SOCs) working in silos are ineffective when trying to defend an enterprise. Consolidating SOCs and coordinating their efforts will improve overall incident detection and response. OMB states that only 47 percent of agencies can detect encrypted exfiltration incidents, and only 27 percent have the ability to detect an exfiltration attempt. Consolidation is part of the solution but detecting the exfiltration of data by a SOC across an agency, especially a Federated agency requires more than consolidation. A SOC must have the right tools in place to tag and monitor the activity of sensitive data on an endpoint, server, data center, in storage, or in the cloud. A SOC also needs the ability to look into encrypted traffic and scan for sensitive data and malware. If a SOC does detect a data exfiltration threat, the SOC needs to have a solution in place to mitigate the threat, preferably utilizing automation.

Recommendation No. 4: Drive Accountability Across Agencies

I would like to focus on the "data-level protections" aspect of this recommendation. OMB acknowledges the call from industry, privacy advocates, and the GAO for an increased focus on data-level protections. However, the Government must expand the scope of data-level protection to include data-level prevention as well. Far too often we see the Government equate data-level protection with the encryption of data, both in transit and at rest. Encryption is important, but its focus is limited to data "protection." This thinking needs to be expanded to include prevention—specifically "data-loss prevention" (DLP) capabilities that prevent the misuse of data in the first place. DLP solutions can discover where sensitive data lives, categorize the data based on its sensitivity and control who has access to the data. DLP can also enforce policies that describe what can be done with data. For example, DLP can block data from being copied to a thumb drive, emailed to a personal email account, block access to data from certain locations, or during certain times. DLP can even automatically encrypt data before its transmitted even if the end-user forgot to encrypt it themselves.

CDM is slated to address Data Protection in Phase 4 of the Program. I recommend that DHS advance Data Protection so it is implemented concurrently with on-going and planned CDM Task Orders. This would have the added benefit of maximizing the effort undertaken by agencies during the OMB mandated Cyber

Sprint of 2015 and its follow-on components. Under the Cyber Sprint agencies were to identify their "high-value" assets but were not provided with solutions to protect those assets. The Data Protection capabilities of CDM, along with CDMs funding would go a long way toward protecting high-value assets in a timely manner.

CONCLUSION

This committee understands as well as anyone that cyber threats are growing in number and complexity at an alarming pace and that Government agencies continue to be an attractive target. The OMB report takes a clear-eyed and unbiased look at the current state of our cybersecurity preparedness and does not shy away from pointing out areas that need significant improvement, and makes recommendations that build upon proven efforts of previous administrations. I hope my ideas can build on OMB's recommendations and maximize their ability to improve our Government's cybersecurity posture. Thank you for the opportunity to testify before this committee, and I would be happy to take any questions you may have.

Mr. RATCLIFFE. Thank You, Mr. Durbin.

The Chair now recognizes Ms. Fowler for 5 minutes.

STATEMENT OF SUMMER FOWLER, TECHNICAL DIRECTOR, CYBERSECURITY RISK AND RESILIENCE, SOFTWARE ENGINEERING INSTITUTE, CERT, CARNEGIE MELLON UNIVERSITY

Ms. FOWLER. Good morning.

Thank you, Chairman Ratcliffe, Ranking Member Richmond, and all subcommittee Members for this opportunity. On behalf of my team at Carnegie Mellon University's Software Engineering Institute CERT Cybersecurity Program or SEI, I am excited to contribute today and share our research and experience in cyber risk determination.

OMB's May 2018 report as has been noted contains four core recommendations that we believe are excellent steps to improving Federal cybersecurity posture.

Our work at the SEI can build on and enhance these recommendations. Cyber risk management requires analysis and mitigation of two sides, both the threat and of the consequence or impact of risks that occur.

We know that our cyber exposure is increasing as software is embedded in more aspects of our lives and Government operations and our adversaries are using these exposures to launch more frequent and more sophisticated attacks. Understanding these threats is important but cyber risk management is not only about managing cyber attack—failures of technology, breakdowns in governance or process, human errors, and even physical phenomena like natural disasters, are also cyber risks.

Addressing cyber risks holistically requires a resilience approach, a word I was very happy to hear Mr. Ratcliffe using, and that approach focuses on mitigating the impact of any type of disruptive event. Operational resilience is the ability to achieve mission objectives before, during, and after any disruptive event, whether it is a cyber attack or a system failure. Fundamental to operational resilience is identifying and prioritizing assets that are critical to each organization's mission.

Our team at the SEI has codified operational resilience in the CERT Resilience Management Model. We have applied this model in partnership with DHS by assessing over 600 organizations across all 16 critical infrastructure sectors. These voluntary assess-

ments provide organizations with the baseline understanding of their cybersecurity capabilities. The assessment team also provides the organization with resource guides and recommendations on how to make improvements.

The CERT RMM is used as a way to measure capabilities against the NIST Cybersecurity Framework and other industry standards but the operational resilience approach moves beyond checklist compliance, to enable organizations to make demonstrable steps to improve cybersecurity posture.

Most importantly CERT RMM does not require an organization to start a new cybersecurity program. It allows an organization to baseline capabilities and build a road map for improvement that is both complimentary to and improves organization's inputs to Federal programs like the DHS CDM program. CERT RMM also provides a structured way for organizations to identify, analyze, and mitigate the risks of older, or legacy, information technology as was noted in the OMB report as a major concern.

In many cases as the report recommends, depreciated legacy systems will be modernized or moved to platforms like the cloud. The asset management practices in CERT RMM ensure that the highest-priority assets for each organization are addressed first but introducing new capabilities like the Cloud also introduces new cyber risks.

CERT RMM provides structured guidance on the management of supply chain including new ways to continuously measure and manage the risks of third-party dependencies. A holistic resilience approach is especially important as the Government integrates cyber physical systems into the Federal landscape. Cyber physical systems are often built with functionality as a primary goal and cybersecurity as a secondary or tertiary goal at best.

The military and Federal Government are adopting cyber physical systems in areas like medical devices, in VA hospitals, and census collection capabilities.

To mitigate cyber risks, we must address both threats and consequences in a balanced way with the focus on prioritization of assets that are most critical to our mission.

Thank you for the opportunity to participate today and to discuss how we can advance cyber risk determination and management through operational resilience practices.

[The prepared statement of Ms. Fowler follows:]

PREPARED STATEMENT OF SUMMER FOWLER

JULY 25, 2018

Chairman Ratcliffe and Ranking Member Richmond, thank you for the opportunity to participate in this hearing on assessing cybersecurity risk. I am the technical director of cybersecurity risk and resilience for the CERT division, part of Carnegie Mellon University's Software Engineering Institute (SEI)[1], a Department of Defense (DoD) Federally-Funded Research and Development Center (FFRDC). The SEI conducts research and development in software engineering and cybersecurity, working to transition new and emerging innovations into Government and industry. The SEI holds a unique role as a FFRDC sponsored by the DoD that is also authorized to work with organizations outside of the DoD, including engagement across the Federal Government, the private sector, and academia. As such, we have been working with Department of Homeland Security's critical infrastructure protections since

[1] *https://www.sei.cmu.edu/*.

they were established in 2013. Our research, prototyping, mission application, training, and education activities are heavily interrelated and are relevant to a broad range of problem sets, such as protection of the Nation's critical infrastructure and improved software engineering for large-scale systems of systems.

Disruptions of critical functions that are reliant on computer systems are inevitable. No organization, government, or agency can anticipate every disruption or prevent every cyber attack. Agencies must be able to anticipate and respond to changes in their risk environment at a moment's notice. Furthermore, despite these disruptions, organizations should be capable of continuing operations and meeting mission goals.

We at the SEI applaud the work of the Office of Management and Budget, detailed in the May 2018 report "Federal Cybersecurity Risk Determination Report and Action Plan." As a high-level assessment of Government cybersecurity risks, the report identifies four core actions that I believe will indeed, done correctly, mitigate a significant number of cyber risks across the Federal agencies.

Notwithstanding, there are some finer points, not included in the report that are worth discussing and implementing. First, the report concentrates on only one half of cyber risk management. In order to successfully execute cyber risk management, agencies must ensure they analyze and manage cyber risk or threats as well as the potential impact of the cyber risks and threats on their organization. While the report concentrates on the threat of cybersecurity and proposes better understanding of the cyber risk, outlining the potential effect of any realized threat requires just as much effort.[2] If agencies are to achieve the ability to complete their mission no matter the cyber threat, it is imperative that we manage both the cyber threat and the consequences of the attacks.

Accomplishing this continuity of operations requires a resilience approach to cybersecurity—an integrated, holistic way to manage security risks, business continuity, disaster recovery, and IT operations, executed in the context of each organization's mission and strategy.

Second, by the report's own admission, it does not cover older, legacy information technology (IT) or workforce challenges. Both legacy IT and the workforce shortage are significant and must be addressed if the Federal enterprise is to understand the current cyber risk environment and credibly prepare for the future.

The SEI's Enterprise Risk and Resilience research includes advancing cyber risk management and enhancing it via the planning, integration, execution, and governance of operational resilience. We leverage our research to develop best practices, resilience management models, tools, and techniques for measuring and improving enterprise risk management and operational resilience in the form of actionable guidance for the DoD and Federal civilian agencies.

OPERATIONAL RESILIENCE

Operational Resilience is the ability to continue to operate, and to meet the organization's mission, in the face of evolving cyber conditions. In the ever-changing cyber and technological landscape, organizations need techniques that allow people, processes, and systems to adapt to changing patterns. These patterns include the incessant introduction of both unique threat actors and the means by which systems are exploited. Operational resilience is obtained by ensuring your cyber risk management takes into account both the threat and the consequences of cyber risk.

Cyber risk management, as proposed by the report, is a process to identify, analyze, dispose of, monitor, and adjust approaches to handling threats. Yet we know cyber risk management alone is not enough to ensure that we are prepared to address current and emerging threats. The concept of risk management must adhere to formula between likelihood of threat and consequence of impact.

At the SEI we have found cyber risk is best managed by determining potential impact first. This requires articulation of mission, enumeration of critical services or activities to achieve mission, and asset management.[3] Once critical assets are identified, then we can walk back toward a list of specific threat types and threat actors. Cyber professionals whose efforts are concentrated in the assessment of threats are often doing very good cybersecurity work; however, without consideration of impact and asset management, they may not be protecting the assets most critical to that particular organization. Focusing on mission objectives and critical assets creates operational resiliency in an organization regardless of the source or

[2] As reinforced in NIST 800.39, Managing Information Security Risk Organization, Mission, and Information System View and NIST 800.37, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach.

[3] Asset management is a collection of practices to identify and prioritize the people, processes, data, technology, and facilities required to execute the activities.

type of threat. This focus on mission context also improves the ability to communicate risk, ultimately helping to address finding No. 4 in the OMB report.

Examining consequences helps organizations to identify and mitigate operational risks that could lead to service disruptions before they occur. Organizations can then prepare for and respond to disruptive events in a way that demonstrates balance of command and control of threat mitigation, incident response, and service continuity. Finally, by establishing a robust understanding of assets, agencies can prioritize investments needed to protect, respond, recover, and restore mission-critical services and operations after an incident and within acceptable time frames.

Considering impact is key for comprehensive cyber risk management leading to resilience. If an agency looks only to malicious threats to operations, it risks missing 17 percent (1 in 5) of overall data breaches, which are the result of human error. In the health care and information industries, these errors are much higher at 35 percent and 26 percent respectively.[4] Organizations cannot overlook the role of humans in the management of cyber risks. A malicious act of deliberate sabotage or the unintentional actions of a confused system operator can both lead to a profound disruption. A resilience approach is agnostic of the type of disruption and enables the organization to plan for, avoid, detect, respond to, and recover from incidents including natural disasters, human error, or malicious cyber attacks.

Furthermore, in today's ever-increasing global economy, many organizations depend on external entities for information and technology, increasing the potential risk to their missions and key services. These third-party entities are an extension of the organization and are often given a trusted place in the management of systems and processes. When trust in an external entity is misplaced or misused, the consequences can be significant. Examples include breaches due to a third party's failure to protect data, poor integrity of hardware and software deployed within an organization, or malicious use of trusted extrinsic relationships to gain access to or harm the organization. Agencies must approach the management of supply chain, also called third-party or external dependencies, with a risk-based approach. This approach includes adopting new ways of continuously measuring and managing the risk from external dependencies.

Additionally, agencies can and should determine the maturity of their external dependencies-management practices. Guided by specific service-level agreements, which establish meaningful measures of cybersecurity performance, agencies can better understand and manage the capabilities of their external dependencies, thus increasing organizational resiliency. For example, external dependencies management is especially critical as the Government continues to modernize its IT capabilities using cloud service providers.

Last, for true operational resilience, agencies must move beyond simplistic checklist compliance or penetration testing and take demonstrable steps to improve cybersecurity posture. Our team at Carnegie Mellon University has codified operational resilience in the CERT® Resilience Management Model (CERT–RMM).[5] Developed by deriving practical tools and methods from the best concepts that academia has to offer and best practices from the public and private sectors, CERT–RMM has been applied to measure and evaluate organizations of all sizes and compositions. Developed initially in collaboration with members of the financial services community, CERT–RMM has been used more than 600 times by the Department of Homeland Security to measure the cyber resilience across all 16 critical infrastructure sectors. CERT–RMM can also be used as a way to measure capabilities against the NIST Cybersecurity Framework. Enabling agencies both to ensure compliance and to show measurable improvement in cybersecurity posture, CERT–RMM provides a resource guide mapped to several industry and Government standards.

Most importantly, CERT–RMM is a framework that does not require agencies to start over, but allows every organization, whatever its current competence, a way to assess baseline capabilities and develop a roadmap for improvement as an enhancement to cyber risk management. This also enables a way to address the next topic of legacy information technology (IT).

LEGACY IT

Organizations do not have unlimited resources with the option of replacing older systems and software en masse to help mitigate new cybersecurity threats. Most, in both Government and the private sector, have a mix of old and new systems all connected to each other and most likely accessible to threat actors via the internet.

---

[4] Verizon 2018 Data Breach Investigations Report, *https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.*

[5] *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084.*

While layers of safeguards are placed between these systems and the outside world, legacy IT remains a serious concern and has led to many notable cyber breaches despite these defenses. Knowing where the most fragile legacy IT systems are located is essential. Consequently, at a minimum an organization must engage in effective asset management to gain a detailed inventory of IT. Without a valid inventory, accompanied by a network map, it is unlikely any organization could adequately defend itself or have appropriate continuity plans in place. Moving these deprecated legacy systems to a more secure platform, like the cloud, is a valid and appealing option. Asset management practices enable us to prioritize what needs to be moved in order to ensure that our highest-priority assets are addressed first. Asset management practices are key ingredients that allow an analysis of the risk and reward of migrating legacy IT to new operating models such as third-party cloud service providers.

WORKFORCE DEVELOPMENT

It is not a secret; there is a shortage of experienced and capable cybersecurity personnel. Some studies indicate that the global workforce shortage will reach almost 2 million by 2022.[6] Furthermore, Federal agencies face stiff competition from private industry for the limited supply of cyber professionals that do exist. Consequently, organizations need a long-term plan for amplifying their cybersecurity capabilities. Agencies would benefit from an accurate and objective evaluation of their cyber workforce, and with the right methods and technologies, organizations can identify gaps in essential competencies that are unique to their workforce. This allows agencies to make better, targeted, hires as well as continuing education decisions for current employees, resulting in more efficient use of taxpayer dollars. It will take a combination of strategic hiring and developing staff in parallel to meet the need for qualified resources. Programs like Scholarship for Service,[7] which provides tuition and stipends to students studying cybersecurity and related fields, represent a vital pipeline of cybersecurity professionals for the Federal Government. Agencies should leverage these options, along with partnerships and training such as the Carnegie Mellon University CISO Executive Certificate Program or incident handling courses, to maximum advantage in their workforce development strategies.

Additionally, we need to make cybersecurity an integrated part of our educational curricula starting with our youngest students. Following the 2007 cyber attacks that crippled dozens of its government and corporate sites, Estonia evolved its approach to cybersecurity to include robust educational programs at all age levels and is now recognized as having the best cybersecurity in Europe. In 1961 our Nation committed to a dramatic expansion of our space program with a goal of being the first nation to land a human on the moon. Similarly, addressing our cyber risks with the goal of a Federal Government that is resilient against current and future cyber disruptions requires a National initiative to prepare our workforce. It is essential that we commit to research in emerging areas like artificial intelligence, autonomy, and data analytics methods, and the corresponding training, that will advance our cyber risk management practices in the future.

CONCLUSION

Cyber risks are not unlike other risks that organizations face. Constrained by limited resources, we must mitigate cyber risks by addressing both threats and consequences in a balanced way. The goal is to ensure that we are operationally resilient, preserving the ability to achieve our mission, despite any disruptions, such as cyber attacks. To be resilient requires us to understand and prioritize our assets, including technology, data, facilities, as well as people and processes, so that we can invest in the protection and continuity of the assets most critical to our mission. This is a fundamental concept in operational resilience practices that will enhance Federal cyber risk management capabilities.

Addressing these challenges and the actions listed in the report is even more necessary as we address the integration and risks of cyber physical systems (CPS) in the Federal landscape. Cyber physical systems already exist in manufacturing, health care, automotive systems, and financial services to name a few. These CPS systems were often built with functionality as a goal and cybersecurity as a secondary or tertiary consideration at best. The U.S. military and Federal Government are also integrating CPS in areas like medical devices in VA hospitals, internet of things capabilities in the U.S. Mint, or census collection activities. These capabilities

[6] *https://iamcybersafe.org/gisws/*.
[7] *https://www.sfs.opm.gov/*—CMU–SEI is a participating institution.

present new attack surfaces for our adversaries and require that we advance our cybersecurity risk management practices with a focus on operational resilience.

Thank you again for the opportunity to participate in this hearing and to discuss how we can better address cyber risks through operational resilience practices.

Mr. RATCLIFFE. Thank you, Ms. Fowler.

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

STATEMENT OF ARI SCHWARTZ, MANAGING DIRECTOR OF CYBERSECURITY SERVICES, CYBERSECURITY RISK MANAGEMENT GROUP, VENABLE LLP, TESTIFYING ON BEHALF OF THE CYBERSECURITY COALITION AND CENTER FOR CYBERSECURITY POLICY AND LAW

Mr. SCHWARTZ. Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to appear before you today to discuss our views on the Federal Cybersecurity Risk Management.

I do so in my role as coordinator of the Cybersecurity Coalition, the leading policy coalition of companies that develop cybersecurity products and services.

These issues before us today are not new. Twelve years ago, I was on an advisory board, the Information Security Privacy Advisory Board that NIST hosts, and at that time the chairman of the Government Reform Committee was Tom Davis at the time, would give grades to Cabinet agencies on how they were doing on cybersecurity.

We had before our advisory board the deputy CIO of one agency that had consistently failed for the past 8 years and so I took this time, and this deputy CIO was actually retiring from Government service at that time, so I thought that this was a good opportunity to hear from him directly as to why Government agencies continued to fail. I asked the question you know, what would it take for you to do to succeed?

He said, "Well you know, one time many years ago I got a D, right? We got a D and no one paid attention to that at all, so we are better off failing, right? We can get resources if we fail. If we use the resources that we are given, the best we are going to do is a D or a D-minus. So what good is it for us to try and play to the tests and try and pass these tests as opposed to fail, right?"

This was a security expert that knew what he was talking about in the security space but had no incentive to do what Government was pushing him to do. I think those incentives have changed in terms of the policy space but not in terms of the leadership space and not in terms of getting the attention and getting the resources needed to actually fix the problems.

We have seen that the move to risk management I think helps agencies to tailor the test themselves so that it is based more on risk to the particular agency as opposed to the basic checkbox that we used to have, much more so and under the old FISMA guidance before the reform FISMA of 2014 came forward.

OMB suggests in their report that came out in May that the goal should be to empower the CIO. This has been done for years and years and has not succeeded. Instead we should do exactly what

Mr. Chairman, you suggested in your opening statement, which is to make sure that we hold the leadership accountable.

The Trump administration in their Executive Order says that that is their goal to hold Secretaries and deputy secretaries directly responsible for what happens at the agency in terms of cybersecurity but the CIOs themselves have many, many jobs to do and security is only a small part of what they do.

Instead we should move to do what has been happening in the private sector which is to have the CISOs report to the leadership directly themselves and make sure that the CISOs have some ability to influence the policy and make sure that then the leadership when they are asked questions from above that they have the ability to go to the CISO and hear things directly from them.

The question is now, how do we hold that agency leadership accountable and we make it so that there is a reason to pass and to do the right thing in this space? From my experience I would suggest that having the director of OMB responsible for making sure that agency heads are paying attention this issue as a central mission issue, right? When people don't become the Secretary of the Interior or the Secretary of Agriculture or others, in order to do cybersecurity but you still have to make it part of their mission to do so.

That is going to take OMB, that is going to take the White House chief of staff, making these calls and making sure that it is not just an incident that gets the attention of the Secretary but that it is on the radar all the time. You can also do this at the deputy director level with a deputy director of management and making sure that they are the ones making the calls.

Of course, Congress in your regular oversight of agencies, when you have those Secretaries and deputy secretaries in front of you, you can ask these questions, at other hearings as well and make sure that they are being held responsible for what is happening at the agencies.

Now, is the time to make sure that the agencies are being held responsible for their failures and rapidly addressing these known risks.

I thank you for again for having me today. I look forward to your questions.

[The prepared statement of Mr. Schwartz follows:]

STATEMENT OF ARI SCHWARTZ

JULY 25, 2018

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, I am Ari Schwartz. Thank you for the opportunity to appear before you today to discuss our views on the Federal Cybersecurity Risk Determination Report and Action Plan. I do so in my role as coordinator of the Cybersecurity Coalition, the leading policy coalition of companies that develop cybersecurity products and services.[1]

[1] About the Center for Cybersecurity Policy and Law and the Cybersecurity Coalition: The Center for Cybersecurity Policy and Law is a nonprofit (501(c)(6)) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry including members of civil society and Government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices. The

Continued

Over the past decade, the Federal Government has steadily moved away from "check box compliance" mandates to a risk management approach to address cybersecurity issues. Major steps in this move have included:

- The Cybersecurity Cross Agency Priority (CAP) goals,[2] which ensured that agencies would receive individualized review of their risk management plans;
- The Federal Information Security Modernization Act of 2014,[3] which provided authorities to increase risk assessments of agencies;
- The Cybersecurity National Action Plan, which created a Federal chief information security officer (CISO) at the Office of Management and Budget (OMB); and
- Perhaps most notably, the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[4] which required Federal agencies to utilize the NIST Cybersecurity Framework[5] to establish a process to manage risk and holds agency heads accountable for doing so.

A risk management approach offers each agency the ability to focus on their specific needs and enables them to demonstrate growth in their cybersecurity efforts while taking steps to address the most critical threats to their mission.

OMB's May 2018 Federal Cybersecurity Risk Determination Report and Action Plan shows that, despite some limited progress, agencies have a lot more to do to effectively manage cybersecurity risk.

This is not an unexpected result. Agencies are not adequately resourced to manage cybersecurity risk, and do not have proper cross-departmental coordination processes to identify and resolve any barriers to achieving this goal. The Federal Government has not prioritized cybersecurity risk management and simply changing policies to help agencies measure risk will not change their policies on its own.

So what will change agencies' approaches to cybersecurity risk management and drive real improvement? The May 2017 Executive Order had the right idea. It is up to OMB and the President to hold agency leadership accountable to improve.

The OMB Report suggests that chief information officers (CIOs) are not empowered to make the necessary changes and suggests that leadership should empower them to do so. While that is one approach that seems to have worked for some agencies, we would recommend that to really make a change in agencies, senior leadership needs to oversee cybersecurity risk management. In other words, security officers should not be reporting to the CIO, but to the deputy secretary or the Secretary. A similar move has started to take place in private companies where CISOs are no longer reporting to CIOs but to CEOs or COOs or directly to the Board of Directors. This shift in thinking has happened because CEOs and Boards of Directors have felt pressure to improve cybersecurity at companies as the result of countless breaches and incidents that have created real and material risk that simply cannot be ignored or delegated to only the information technology teams.

For this to work in the U.S. Government, the director of OMB, the White House chief of staff, and the President must hold the Secretaries directly accountable for cybersecurity risk management at the agencies. Similarly, the deputy director for management at OMB must hold the deputy secretaries accountable. Congress must adequately resource agencies and hold the leadership at all levels accountable for managing risk through public oversight. Without this accountability, other measures, however well-intended and necessary, will not be able to succeed to the extent needed to secure our Government.

At this point, every agency's leadership has been told that they are responsible for the cybersecurity of their agencies. Agencies have now been measured and have not fared well.

Center hosts several initiatives focusing on a range of critical cybersecurity issues, including the Cybersecurity Coalition, Better Identity Coalition, and the Hardware Component Vulnerability Disclosure Project. The Cybersecurity Coalition brings together industry-leading companies to share their expertise and unique perspective on critical policy issues, both in the United States and internationally. The Coalition is focused on several active and critical policy issues that require close alignment and coordination to protect the vital interests of the cybersecurity products industry, including: Promoting responsible vulnerability research and disclosure; promoting effective privacy processes within cybersecurity policy; establishing Government requirements for agency systems; increasing information sharing and threat intelligence; and promoting sound cybersecurity practices in government at all levels. Coalition members include Arbor Networks, AT&T, CA Technologies, Cisco, Citrix, Cybereason, Intel, McAfee, Mozilla, Palo Alto Networks, Rapid7, Red Hat, and Symantec.

[2] See Obama Admin. Archives, Cross-Agency Priority Goal Cybersecurity, available at *https://obamaadministration.archives.performance.gov/content/cybersecurity.html.*

[3] Pub. L. 113–283.

[4] Executive Order 13800.

[5] Nat'l Inst. of Standards and Tech., Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (2014).

Now is the time to hold the agency leadership responsible for failures and to rapidly address these known cybersecurity risks.

Mr. RATCLIFFE. Thank you, Mr. Schwartz.

I now recognize the gentleman from New York, Mr. Donovan for 5 minutes.

Mr. DONOVAN. Thank you, Mr. Chairman.

Thank you all for sharing your expertise with us but to show you how I lack expertise I have a VCR back home it still flashes 12 and you cannot see because you are facing us but all the young people behind you now, Googling, "What is a VCR?".

So just so I can understand the problem properly, if we are protecting our gold in Fort Knox and there is only one entrance in there, we have a good chance of making sure anybody who gets through there is a person that ought to get through unless they are disguising themselves as someone else and I guess in your field you would call that just looking like a friendly user to get into a network when you are actually an infiltrator.

The difficulty is when you have more than one entrance I guess or if you have secured your entrance but there are other people who have entrances and are not securing it as well as you are, that causes vulnerabilities in Fort Knox and causes vulnerabilities in systems I suspect because it was hard for me to grasp before I joined this committee on like, why cannot we just protect this?

If we know, as much as the bad guy, do we anticipate what they are going to do? I think Ms. Fowler you used word resiliency and the Chairman used the word resiliency.

Before we have a tragedy or an intruder so could you kind-of like frame the problem for me so I could understand it because I think I have to understand the problem before we could actually come up with or understanding what your suggested solutions are?

Mr. DURBIN. OK. Thank you for the question. It is a complex situation, a lot of it has to do with the diversity of the Federal Government, the diversity of the agencies, how they are organized, some are more flat, some are federated, some have more resources than others do so it is coming up with a common baseline of what is it that we have and what is it that we are trying to protect.

I believe that the CDM program in their Phase 1 certainly is trying to fix that situation by doing that definition. Phase 1 the goal is to go out and identify all hardware and software assets because some have made the comment and it is very true, you cannot defend what you cannot see.

So now that we are closing in on the end of Phase 1, we will have a much better look at what it is we are trying to defend so that we know, what all those different entry points are that you referred to and then we can work on providing protections against all of those different attack vectors.

The other issues are legacy systems that we have talked about. You have a disparity between different people's products and solutions that they are using for access management or for determining who is qualified, who has privileges to access a certain system and should they have those accesses so a lot of this needs to be discovered and baselined so that we have an understanding of what the problems are and then we can come up with solutions to solve them.

Mr. DONOVAN. Thank you.

Ms. Fowler.

Ms. FOWLER. Yes. I am excited to hear you use the word resilience because it really is about resilience. When you use the example of gold that needs to be protected, it is not even just against someone who trying to steal that gold but when we think about the fact that the gold is housed somewhere, it is in a container could it be impacted by a natural disaster, could someone who is working there make a mistake, and that would also cause us to lose our ability to access or use that gold.

So we really want to look at this from a holistic standpoint of not just trying to figure out what it is that an adversary is trying to do but to understand what it is that is most important to us and how we can ensure that it will not be impacted in any negative way, right? From any sort of disruption.

That really even starts before understanding what our assets are and that is related to what we talked about with having leadership have a real skin in this game. It is being able to articulate and communicate what it is that we are trying to achieve from a mission standpoint so you know, organizations like Health and Human Services and Department of Energy have different missions that they need to achieve, they have different services that they are going to provide to achieve those missions, and then the assets that support those services are what we really need to protect. So it is the identification of the assets that are important to each mission.

The way we can use the limited resources that we have best is to be able to articulate our risk appetite against those assets that are in our organizations and make sure that programs like CDM are focused on those.

So you know, my way of explaining this to you would be, let us not just look at this in terms of a threat from a cyber attack but a holistic, how do we protect against the impact of any negative consequence?

Ms. Fowler, thank you.

Mr. Schwartz.

Mr. SCHWARTZ. You talked about protecting the gold in Fort Knox but that reminds me of a saying that they use in the military about "protecting diamonds and toothbrushes" which is, if we were to protect diamonds the same way as we protect our toothbrushes, we would have a lot of toothbrushes and not very many diamonds.

That is part of what both Mr. Durbin or Ms. Fowler are discussing here, which is how do we do risk management in this space, in a way where we can identify the assets and then do the risk profile in a way that makes sure that we are protecting that information in the right way that it needs to be protected?

Prior to the NIST framework, the NIST Cybersecurity Framework, which Mr. Durbin mentioned, the Federal Government actually pretty much just had a list of the things you need you for every system and did not really take the less important systems or more important systems and kind-of do that balancing test of how should we be protecting this particular system.

Now we are moving toward a time when we are doing that kind-of risk management and that is what this OMB report's really

about, is how agencies are looking at risk in this space; how are they identifying it, how do they do these different pieces, right?

I break the NIST profile into identify, protect, detect, respond, recover, which I break up into two pieces, one is the defense side so the identify and protect, and then the other side detect, respond, recover I think of as a resilience side, as Ms. Fowler has been saying right?

So that is the how do you get to do both sides of that and make sure you are doing it the right way for each system and that is the kind of approach that now agencies are taking for the most part but they still have problems in terms of actually putting the protections in place, actually making sure that they are resilient in the way that they need to be even for the most critical systems.

Mr. DONOVAN. I thank you all again for your expertise.

Mr. Chairman, I yield back, which time I don't have any more.

Mr. RATCLIFFE. Well, thank the gentleman.

The Chair recognizes the Ranking Member, Mr. Richmond—the Chair recognizes my friend and colleague from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I thank the Ranking Member.

Thank the panel also for their testimony today, the expertise, the insights that you bring to these challenging topics.

Let me begin if I could with Mr. Schwartz, you spoke of the need to hold Secretaries, not CISOs accountable for the security of their agencies' networks and I certainly would agree.

I remember what happened when a Secretary of Defense Ash Carter started taking a deeper interest in this topic and doing a deep-dive requiring weekly reports being given to him and even on the issue of establishing a Bug Bounty Program when he said, "We are going to make this happen," he started telling people and programs to get out of their way and make it happen, it did.

So I can see the why it is so important to have Secretary buy-in but you know, it seems that for years poor results on FISMA scores have not been enough in other agencies though to motivate action.

So my question is what could the administration do to encourage real action to address these continued deficiencies and ensure cybersecurity leadership at the highest levels and again from your perspective why is it so important to have Secretarial buy-in?

Mr. SCHWARTZ. Thank you, Mr. Langevin. Thank you for your continued leadership on these issues too.

I think there is a lot in that question in terms of, how do we get leadership to actually focus on this?

I do think that the executive—or the Trump Executive Order that came out in May 2017 actually put us in the right place, which is before the Secretaries had all of their goals in place they were told that cybersecurity was a major issue.

But it takes staying on top of that to do that. That means holding Cabinet meetings around cybersecurity and the President going around and asking each agency what they are doing, holding up the report card from OMB and asking them, "What are you doing to do more," right? That is what really taking the Executive Order and actually implementing it means in this space.

I realize that there are a lot of other things going on but that is what is going to make a difference in this area, is making sure that the Secretary knows that they are going to be going into a meeting and that they have to prepare for it and the 50 people that follow them around and do every day and do that thing for that day, this is going to be the thing that we are doing today, right?

Therefore, everything needs to be in line and we need to get the CISO in front of us so he can give us the answers of what we need——

Mr. LANGEVIN. Yes.

Mr. SCHWARTZ. Rght? That is the only way that it is going to change.

This is the same thing that is happening in the private sector too, not every company is doing this, those that are, are more successful.

Mr. LANGEVIN. Yes. Yes, I would agree. I mean, if the top people are not paying attention to this then clearly it becomes a secondary priority but the President or the Cabinet Secretaries are the ones that are driving this then clearly everyone's going to stand up, shine the shoes, and get this done the right way.

So, Mr. Schwartz, on another issue with small- and medium-sized businesses have largely resorted to outsourcing not just their IT but also the security of their IT given their limited budgets. In a similar vein the OMB report suggests that shared services are key to addressing risk management issues, yet we have made little progress to that end.

So Mr. Schwartz, if you could, what barriers do agencies face in getting to shared or outsourced services and how do we overcome them?

Mr. SCHWARTZ. Yes. The shared services one is a tricky problem for a lot of agencies. Part of it is just the culture of the fact that they have had been doing internal security for years and years and they have to move away from that and spend the money on the cloud company doing the protections for them rather than keeping that same security in-house.

The small agencies in particular, those that don't even have a large IT department are never going to be able to have enough security professionals and technology to protect themselves, whereas the cloud companies specialize in that, the managed security services specialize in that so there is a need to move in that way.

I think the main challenges that they face are really procurement challenges though because you know, you want to do oversight of the agencies that you are in charge of doing oversight over. If they are turning over a lot of their budget to other agencies in order to run their services, you lose oversight over their IT, right?

I understand that from a Congressional point of view but that is how we are going to improve with the small- and medium-size agencies, is by Members of Congress understanding that and being willing to take the risk of saying, "OK, we understand that you are going in someone else's purview, we are losing some control here."

But we know, that that agency has security in place and that they have oversight over what they are doing as well, and our information being held by that agency and being overseen by compa-

nies in that space that run the managed services in that space is going to be acceptable.

Mr. LANGEVIN. Very good.

Thank you for those answers. As you can imagine I have several more but time is expired.

So I will yield back. I will have some questions to submit for the record unless we go to a second round.

Thank you. Thank you all.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes the gentleman from Nebraska, Mr. Bacon for 5 minutes.

Mr. BACON. Thank you, Mr. Chairman. I appreciate it. Thank you for coming in here and sharing your expertise.

I used to work in the cyber offensive side a little bit, cyber intelligence side, and we have some of the best capabilities in the world there but we were also the most vulnerable when it comes to defense and other people cyber attack. I heard a cyber leader once describ us as living in a big glass house and we had the biggest rocks, not very comforting at times.

One of the things that the OMB and DHS report calls for is the consolidations of the Security Operations Center and instead of each one having their own by consolidating it to one big one, do you see that as a significant advantage or does having this does it make everybody equally vulnerable if you get into one, you get in everybody?

So I would like to have your thoughts on that. Thank you.

Mr. DURBIN. Yes. Thanks for the question. So having a SOC for the sake of having a SOC may not be the best strategy. It comes down to your ability to stand up a SOC that has the right tools and capabilities to accomplish what it is you are trying to do.

So if you are in a position where it would be better for you to merge with somebody else's SOC that has proven technologies and has the access capability that might be the better way to go so I agree with the recommendation of the report, the consolidation of SOCs will improve some efficiencies.

Mr. BACON. So it gives the best capabilities available for everybody——

Mr. DURBIN. Exactly. Yes. Now——

Mr. BACON. It standardizes the best——

Mr. DURBIN. Yes.

Mr. BACON. OK.

Mr. DURBIN. Yes and of course you need to make sure that you consolidate to a SOC that does have the excess capacity and that does have the tools in place——

Mr. BACON. Right.

Mr. DURBIN. That are going to accomplish the mission.

This recommendation was also made around the idea of improving the ability to detect data ex-filtration and simply consolidating SOCs may not accomplish that. You know, the SOC has to have the right tools and to be able to discover where the data lives and tag that data as sensitive so that you can then monitor——

Mr. BACON. But by consolidating we can invest in that one and make sure that we have the best capabilities——

Mr. DURBIN. Exactly.

Mr. BACON. I would say, but would you all just agree?
Mr. SCHWARTZ. Agreed.
Mr. BACON. OK.
Ms. FOWLER. Yes.
Mr. BACON. Are we doing better Mr. Schwartz, when it comes to sharing intel data because we don't have a lot of silos. I mean, you touch on this with Mr. Langevin a little bit but are we doing better making progress?
Mr. SCHWARTZ. There is some progress there. I think a lot of the private sector is still really frustrated. A lot of it comes down to getting security clearances and the right people getting the information so I still hear a lot of frustration.
I think internally inside the Government it has gotten a lot better though——
Mr. BACON. It seems to be having a combined security operation center allows you to share that data faster because you can see where there is infiltration or ex-filtration.
I had a just a question Mr. Durbin because this fascinates me. Evidently, you have talked about a group, well, let me just read it here, "Symantec has engaged regarding a new attack group known as 'Thrip'," and the ways in which they are living off the land in order to get info systems," can you talk about this new threat and living off the land, what does that mean and what kind of a cyber threat is this?
Mr. DURBIN. So living off the land is how we are describing a technique where if an attack group creates a complex sophisticated piece of malware that they use to infiltrate a system, it is going to be relatively easier to detect that because we haven't seen it before, it doesn't look right, it raises a flag so if an attack group can utilize a network administration tool that administrators commonly used to scan networks to see what they have and somebody sees that activity inside the network it is not going to raise a flag——
Mr. BACON. It's camouflaged?
Mr. DURBIN. Yes, they could say, OK, well somebody's just scanning the network because that is part of what they do——
Mr. BACON. Right.
Mr. DURBIN. So that—and that is just one example using PowerShell scripts and things, is just ways to mask their abilities so it is not as easy to detect.
Mr. BACON. It makes sense.
One last question, I know, the Russians use a lot of phishing techniques, that is how they entered the DNC server. It seems to me that makes us the most vulnerable, is that technique. What can we do to better defend against these phishing techniques that are going on?
I will just open up to whoever feels like they have the best answer.
Ms. FOWLER. Go ahead.
Mr. SCHWARTZ. I would say getting better identity management is really the key to the phishing techniques. I mean, right now, a lot of times we still rely on username, passwords, and moving toward techniques that move beyond that.
They talk about that a bit in the report that there has been a move toward use of cards sort-of which I think does help to some

degree inside the Government but it is really about the credential and whether you can secure that credential.

Ms. FOWLER. We absolutely do see phishing as one of the most common vectors for having attacks occur. A couple of things that we need to do.

One is training although we know, that no matter how much we train people over and over it takes just one person to hit the link and cause the issue to occur so thinking about advances in terms of automation and analytics and the things that we are doing in the areas of Machine Learning.

So this is going to take us advancing past our adversaries' capabilities and investing in the research that will get us there.

Mr. BACON. Thank you, Mr. Chairman.

Mr. RATCLIFFE. The Chair now recognizes my friend from Louisiana, Mr. Richmond.

Mr. RICHMOND. Thank you, Mr. Chairman. I think you touched on it a little bit but from my perspective, when it comes to Federal network security I see at least two systematic problems but they stem directly from the White House, one of which is the tendency to undercut or diminish the role of authority figures, eliminating the cybersecurity coordinator is a good example.

Second, it is taking far too long to fill senior positions like chief information officers and at the end of last year nearly one-third of the agencies were still operating without a permanent CIO and the Federal CIO was not named until January and the Federal CISO was selected just last week.

How important is strong, clear leadership structures when it comes to cybersecurity particular for an agency trying to instill a culture of risk awareness? I know, Mr. Schwartz you mentioned having a chief executive that will hold people's feet to the fire, the question becomes can that be delegated and without a cybersecurity coordinator, where do we find ourselves?

So anyone can answer that, let us start with Mr. Schwartz.

Mr. SCHWARTZ. Yes. I have always felt that the cybersecurity coordinator should be I mean, it should be brought up to be a deputy level.

There was a commission, the Obama Commission that was preparing for the next President, suggested that it be raised to an assistant to the President but I actually think it makes sense to have it at the deputy level particularly for the reason of being able to call out deputy secretaries on these kinds of issues and make sure that they are held accountable.

Getting rid of that position totally I think is a step backward from being able to do that. I mean, you can have a deputy play that role but they are going to have 90 other jobs, right? So how much time can they actually spend calling up deputies and asking them how they are doing on cybersecurity or if you are supposed to be having someone dedicated toward just doing, offensive capabilities, defensive capabilities inside the Government as well as critical infrastructure protection too but having this one piece be part of their job as a deputy at the level of deputies I think makes a lot of sense.

So again, I think that they took a major step backward by getting rid of the position totally rather than elevating it the way they should have.

Ms. FOWLER. I agree that governance and leadership are the most critical first step in establishing good cyber risk management practices. It is also a matter of making sure that the work force itself who is in those positions are trained in these areas and understand how to manage cyber risk like other risks are managed.

We often look at cybersecurity as something that is special or not understood and really, we need to manage cyber risk like we manage other risks inside of the organization and that is a matter of using those limited resources in the best way possible.

So the leaders that we do put in place it is incumbent that they set that risk appetite and understand what the tolerance ranges are for that organization and communicate those to the work force.

The work force is doing the absolute best that they can to do all of the right technical things, it is just ensuring that they are provided the guidance that it is going in the right step so the governance aspect of this is that most important first step.

Mr. DURBIN. I would just simply add that no matter what cybersecurity program you are trying to set up, it is key to get buy-in from all levels of the organization and that is no different with the Federal Government.

Mr. RICHMOND. Let me ask this because I think that it also came up but the Federal Government's always lagging behind the times and we are about 10 years back from where we should be in terms of our cybersecurity.

How can Congress empower or provide the resources for our Federal agencies to actually be proactive and better prepared for the future and then anticipate the risk as opposed to always been on the back end?

Ms. FOWLER. So I will speak to that in terms of what I think is required for us as a Nation to move forward and you will see in the written testimony, I think this requires a National initiative to address cybersecurity as a need across all sectors.

You know, in 1961 we made this goal to put a human being on the Moon and that sparked interest in a whole lot of different science and technology that was developed. We need to have a similar initiative which goes down into our education levels at all levels starting very early which makes this a part of every level of education so that the work force in the future is prepared for this.

We saw this with Estonia when Estonia experienced their crippling attacks, that Government decided to really put the initiative forward to educate across all levels of their citizenship and now, they are recognized maybe arguably but as the No. 1 in cybersecurity in all of Europe.

I see that we need to put forth an educational initiative that will prepare our work force for this in the future.

Mr. RICHMOND. Thank you. Thank you. I see that my time has expired so I will just yield back.

Mr. RATCLIFFE. Yes. Let me give you all—first of all, the Chair recognizes himself for questions.

Ms. Fowler, I very much appreciated your remarks there and I agree. I have talked about a cyber moonshot and identifying an ap-

proach that will address some of the concerns that you related and if you believe as I do that cybersecurity risks present perhaps our greatest National security threat right now and going forward then we need to have some sort of a cyber moonshot to address those threats.

But I want to give each of the witnesses a chance to weigh in on the Ranking Member's very good question, one that I had as well.

So Mr. Durbin.

Mr. DURBIN. If you were to take a look at the original CDM documents 5 years ago and look at the projections of where they thought they would be by now, we would be in much better shape.

There are reasons why we are not there yet. Phase 1 is a critical phase, it builds the foundation. We basically had told the agencies let us know, give us an inventory of all of your assets so that we can then turn around and provide you with a tool that is going to give you an accurate inventory count.

So there was no shock when after Phase 1 was deployed and that tool was turned on, the number of assets in the agencies was found to be severely under-reported.

That is a good thing. It is a good thing that we now have visibility into what it is we are trying to protect so that took more time than they originally thought.

So if we were to accelerate the other phases and let us get to the point where we can automate the authority to operate process, every 72 hours we are doing a scan, so an organization knows you know, am I able to operate, do I have some deficiencies that need to be repaired in kind-of real-time, I think that would put us in a much better position.

They did add Data Protection as a Phase 4. I applaud them for that but that is what the bad guys are after. They are after the data so while we are trying to figure everything else out, let us protect the data, let us lock that down.

Mr. RATCLIFFE. Perfect. Thank you.

Mr. Schwartz.

Mr. SCHWARTZ. Thank you, Mr. Chairman. This you know, responding directly to your comments on this issue about the cyber moonshot and the threat that comes from cyber and the space compared to other threats. I mean, look at what we have done on terrorism, right?

We have done a pretty good job in terms of trying to resource-out how we protect this country from terrorism but we have been told for the past 7 years that cyber is overtaking terrorism as the most major threat to this country and we are not getting the resources to cyber that we have for terrorism.

So I am not sure that that is a moonshot or what you call it but there is this question of paying as much attention to this problem as to address it in the way that we think of it as the size problem that it actually is.

That is why I focus on you have to have Cabinet-level meetings in order to do that, you have to put the resources toward it that are commensurate with it and we are not doing that now, so we cannot expect to get the results particularly at small agencies in

order to protect themselves when we are not helping them out to do that.

Mr. RATCLIFFE. Terrific. Thank you.

As I mentioned in my opening, the OMB and DHS report that I think the specific number was 71 of 96 Federal agencies have cybersecurity programs that are either at risk or at high risk and a statistic that really jumped out at me as being particularly disturbing and I am wondering if the number surprised you as you read that and whether it does or not.

When we talk about reversing the trend there, I mean, I mentioned CDM as a solution there but I want to make sure that that we are talking about all the potential solutions to reversing that trend and give you all the chance to weigh in on making those points.

Mr. DURBIN. So I guess the percentage did not surprise me all that much given the fact that CDM is behind and that some of the recommendations made in last year's Executive Order are just now starting to take hold so again it did not surprise me.

I do see CDM as a way to fix a lot of what is in that report instead of creating a new program, let us utilize what is already there and let us improve it, let us empower it so that we can target those specific issues and bring that percentage down as quickly as possible.

Mr. RATCLIFFE. Terrific. Thank you.

Ms. FOWLER. I would agree that the 71 is not surprising. It is also consistent with what we have seen through our work with DHS, what the SEI has done with DHS in looking at the private sector with the owners and operators of critical infrastructure.

I would say that CDM in accelerating that program will be help in terms of giving us visibility into what our capabilities are.

Again, I do want to see us move toward an operational resilience approach where even before we start thinking about what it is in terms of a threat actor that we need to worry about that we think about the most critical assets inside of each organization.

Mr. RATCLIFFE. So can I stop you there Ms.——

Ms. FOWLER. Sure.

Mr. RATCLIFFE [continuing]. Fowler because you talk about that in terms of the resilience factor. Are there key metrics that we can be looking at to determine how effective we are being in terms of making progress on resilience?

Ms. FOWLER. Absolutely. We do have something called the "Cyber Resilience Review" which is a set of questions that look across 10 domains of cybersecurity and that can help give a maturity measure of how you are doing in terms of the completeness of the practices and also the institutionalization or sophistication of the practices that you have in place.

The third element of that is something that you yourself mentioned sir, which is efficacy of practice and that is something that has been a concern and continues to be a concern back at the SEI because we can be doing a lot of things very well and they might not be the right things to do.

Much like we do in the medical industry, we set up very scientifically rigorous tests and we do a lot of data analysis behind whether or not those tests work in very specific ways.

We don't have a lot of those practices occurring in cybersecurity to say, "Does this control actually do what we want it to do in the face of this threat?" That is something that I think that the Government could invest research in to make sure that the efficacy of the practices is as good as the completeness of the practices.

Mr. RATCLIFFE. Great point. Thank you.

Mr. Schwartz I will give you the last word.

Mr. SCHWARTZ. Sure. So I mean, I addressed this in my oral testimony but just to take it a little bit further. I mean, what do we do with agencies that are a high risk? Do we spend more money there? Do you give them more money to continue to fail? Do you fire people? So they have less people there to do the job that they need to do.

I think each agency is a sort-of its own case and what we need to do is give people a reason to succeed and make sure that the leadership understands what they need to do to succeed.

Sometimes there are a lot of barriers in the way to success, OK, then you have got to tackle this one at a time and get the right people from the entire agency in order to do that and to address those one at a time but it involves digging in, in each of those agencies and figuring out what the right path to success is.

It is part of what risk management is but it is also just management at an agency at this point.

Mr. RATCLIFFE. Well I want to thank all of our witnesses.

This has been incredibly insightful and valuable for all of us. Thank you all for being here today.

I also want to thank the Members of the committee for their questions and remind them that they can submit additional questions for the witnesses and it sounds like at least one of the Members will and we will ask the witnesses to respond to those in writing.

Pursuant to Committee Rule VII(D), the hearing record will be held open for a period of 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE JIM LANGEVIN FOR SUMMER FOWLER

Question 1. You spoke in your testimony about the importance of understanding the potential effect of realized cyber threats. The 2015 OPM breach exposed a gap in OPM's understanding of the damage that could result from the loss of security clearance records—a risk more consequential to other Federal agencies.

What can the administration do to address cyber risk management holistically, rather than agency by agency?

Answer. The Federal Government is an enterprise comprising departments and agencies with specific objectives and missions that support the larger Federal objective of serving the public. Addressing cyber risks at this level requires an enterprise risk management (ERM) approach. Carnegie Mellon University's Software Engineering Institute developed an ERM process that is targeted at not only managing risks but at ensuring organizational and mission resilience. Organizational resilience is the ability for a department or agency to achieve its mission before, during, and after a disruptive event (such as a cyber attack) and to return to normal operations as soon as possible. Our 10-step ERM process is shown in Figure 1.

FIGURE 1: ENSURING ORGANIZATIONAL RESILIENCE VIA ERM

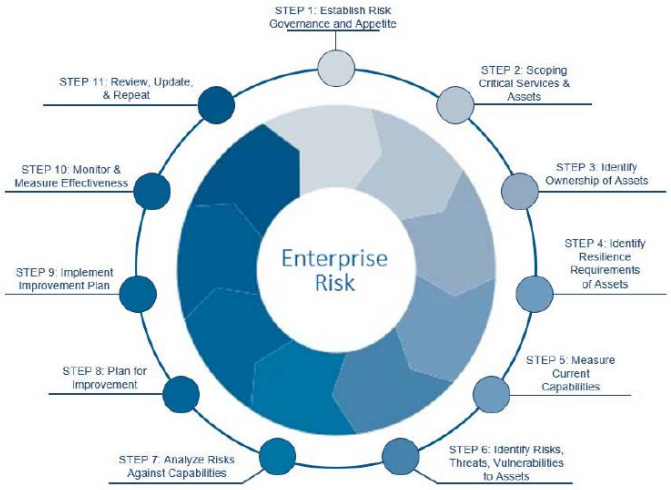


Figure 1: Ensuring Organizational Resilience via ERM

The process must begin by establishing governance, risk appetite, and risk tolerance ranges. This should be done at the top levels of the Federal Government and communicated down to all departments and agencies so that they have an understanding of targets/goals for their cybersecurity programs. This can be daunting at the enterprise level, but it is a best practice that large private companies use to ensure alignment of cybersecurity activities to overall business objectives. While the cyber risks will still be owned and managed at the department/agency level, this

also provides a standardized way for cross-agency dependencies and risks (e.g., risk of OPM data breach to other agencies) to be communicated and managed.

Enterprise risk management addresses cyber risks holistically by first focusing on mission objectives, critical assets, and requirements before leaping to technical solutions. This process also provides a structured way to develop measures and metrics to monitor performance of cybersecurity and cyber risk management practices at an enterprise level.

Unfortunately, if we were to comprehensively answer the question of cyber risk management, detailing each step, our response would likely be too long to be appropriate for this forum. However, both the CERT Resilience Management Model (CERT–RMM) handbook[1] and "The 3 Pillars of Enterprise Cyber Risk Management,"[2] from the Insider Threat Blog, are readily available on-line. Additionally, the SEI is more than happy to schedule discussions with Rep. Langevin and his staff. This invitation is of course extended to any Member and his/her staff.

Question 2. One continuing challenge with prioritizing Federal expenditures on cybersecurity controls is the lack of viable metrics for assessing the effectiveness of those controls in reducing cybersecurity risks.

What are the obstacles to closing that gap so that we can measure the relative value of various cybersecurity controls? How is SEI working to overcome those obstacles?

Answer. Thank you for recognizing and articulating this challenge. Although cybersecurity is viewed as a technically advanced field of study, we are still in our infancy when it comes to measuring efficacy of capabilities. Other scientific fields such as medicine perform rigorous studies following the scientific method with a hypothesis and control groups to determine the efficacy of capabilities. In cybersecurity, we are still relying on subject-matter expertise and compliance as our primary tools for "measuring" capabilities.

The challenge in applying the scientific method is that in any given instance of measuring a cybersecurity capability, there are several factors to consider:

1. The operating environment and its configuration (e.g., a computer server).
2. The cybersecurity control being applied and its configuration (e.g., a firewall).
3. Potential threat(s) and/or threat actor(s) (e.g., criminal hacker).

Each of these factors has multiple possible states that must be tested. This means that testing the NIST 800–53 controls, for example, would require tens of thousands of test cases to account for the various operating environments, control configurations, and potential threats. I have written more about measuring cybersecurity performance in the CERT blog "Cybersecurity Performance: 8 Indicators."[3]

Carnegie Mellon University's Software Engineering Institute is investing a portion of its Congressional Line Item research funding to develop and validate a methodology for measuring the efficacy of a cybersecurity practice. If successful, the community will have a new methodology for measuring the cybersecurity of a system and be able to rank order the importance of the controls needed to protect it. This is a nascent concept and will require additional investment into research and transition into practice, but it is an important step in making scientifically valid improvements in cybersecurity. Future work will use emerging artificial intelligence concepts to automate the methodology and simplify the process.

QUESTIONS FROM HONORABLE JIM LANGEVIN FOR ARI SCHWARTZ

Question 1. Having served on the National Security Council, can you speak to the cross-agency issues that are likely to emerge without a Cybersecurity Coordinator at the White House?

Answer. In 2008, a Center for Strategic International Studies (CSIS) bi-partisan Commission led by Chairman McCaul and Representative Langevin called for:

"An assistant to the President for cyberspace, who directs and is supported by a new office in the EOP—the National Office of Cyberspace. This office would be small (10 to 20 people) and would provide programmatic oversight for the many programs that involve multiple agencies . . .

---

[1] *https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf.*

[2] *https://insights.sei.cmu.edu/insider-threat/2017/11/the–3-pillars-of-enterprise-cyber-risk-management.html.*

[3] *https://insights.sei.cmu.edu/insider-threat/2018/03/cybersecurity-performance-8-indicators.html.*

"Because cybersecurity requires coordination of activities across agencies, the White House is the best place to locate this function. It alone has the authority to ensure coordination. The most appropriate place in the White House is the NSC."[4]

When the Obama administration took office, it created a cyber policy office in the NSC and put a special assistant to the President in charge of this office with the title, White House Cybersecurity Coordinator, reporting to the assistant to the President for Homeland Security and Counterterrorism.[5] At the time, several commentators suggested that this role was ranked too low in the NSC structure given the current and anticipated importance of cybersecurity for the Nation. Nevertheless, this office grew to 10 to 15 people and became an effective structure to coordinate and provide oversight and direction for a wide range of programs and initiatives involving multiple agencies. The office also became a focal point for interaction with the private sector on high-level issues of policy and National security.

Listing all of the successes of the cyber office since its inception would be a considerable effort, but during my 2½ years at NSC Cyber under the leadership of then-Cybersecurity Coordinator Michael Daniel, we coordinated a number of important policies and actions:

- Creation and promotion of the NIST Cybersecurity Framework;
- Creation of the Cyber Threat Intelligence Integration Center;
- The Executive Order on Cyber Sanctions;
- Development of a working Vulnerabilities Equities Process;
- Creation of a standards body for Information Sharing and Analysis Organizations;
- The remediation of the Heartbleed vulnerability and greatly increased speed in patching critical vulnerabilities in Government agencies;
- Agreement with the Chinese government on norms related to corporate espionage through cyber means;
- Agreement among agencies on roles in cyber incident response;
- Implementation of U.S. Cyber Operations Plan (PPD–20), which was drafted by NSC Cyber prior to my arrival;
- Reconstituting the interagency Cyber Response Group (CRG);
- Working with Congress to draft the Cybersecurity Information Sharing Act (CISA), which passed and had implementation coordinated by NSC Cyber after my departure; and
- Sponsoring the successful White House Cybersecurity Summit at Stanford University in February 2015, where companies pledged to move forward on several important joint cybersecurity projects with Government.

While the cybersecurity policy coordination in the U.S. Government is by no means perfect, it improved demonstrably from where it was when the CSIS Commission first made its recommendation.

In fact, in 2016 the bi-partisan President's Commission on Enhancing National Cybersecurity[6] again recommended that the President elevate the current position of Cybersecurity Coordinator to an assistant to the President. The report explains that the position should have responsibility for bringing together the Federal Government's efforts to protect its own systems and data and to secure the larger digital economy, and as well as for informing and coordinating with the director of the Office of Management and Budget on efforts by the Federal chief information officer and chief information security officer in order to secure Federal agencies.

In general, I agree with both commissions that the special assistant role was too low level to be as effective as possible. However, instead of raising the level to an assistant to the President. I would split the difference and suggest that the cyber coordinator be a deputy assistant to the President. This would allow the NSC to work closely with the deputy secretaries to make cybersecurity a lead issue for every Cabinet agency and better create areas of consensus around important new cyber policy, while still providing the ability to raise major policy issues to a higher level when disagreement occurs.

---

[4] "Securing Cyberspace for the 44th Presidency: A Report by the CSIS Commission on Cybersecurity for the 44th President" December 2008 *https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf*. See page 36.

[5] In my time at the White House, it was explained to me that for the NSC: An assistant to the President is the Presidential Commissioned Officer that could run meetings at the level of an agency head or Secretary; a deputy assistant to the President could run coordination meetings at deputy secretary; and a special assistant to the President could run meetings at under secretary or assistant secretary. There were exceptions to this rule but it gives a sense of overall hierarchy in relation to the rest of the Executive branch.

[6] *https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf*.

The current administration has decided against all of these approaches. It has demoted the role of NSC Cyber by not replacing the cybersecurity coordinator and removed the related commissioned officer position entirely. It also has demoted the Homeland Security and Counterterrorism advisor to a deputy. While this may still provide a tenuous hold onto the increased coordination among agencies that was so hard-earned over the last decade, I am concerned that eventually this coordination will decline and the result will be a de-prioritization of cybersecurity as a National security issue. Either there will be a cybersecurity incident that causes confusion among agencies, or the old rivalries and petty squabbles among agencies will return at a time when the White House leadership is not able to organize and offer a consensus path forward.

I find the decision to demote the NSC Cyber particularly frustrating because at the beginning of this administration there seemed to be the possibility that greater progress could be made toward increased coordination.

Question 2. Having been intimately involved with a very successful cybersecurity Executive Order, EO 13636, and the NIST Cybersecurity Framework that came out of it, what is your impression of how agencies are making use of the CSF now that they are mandated to?

Answer. The NIST Cybersecurity Framework ("CSF") was designed to provide standards, guidelines, and best practices to help entities manage cybersecurity-related risk. Conversely, the CSF was not designed to provide a prescriptive set of requirements that must be satisfied in order to achieve a desired outcome. This risk-management approach can be distinguished from the checklist-oriented compliance style that many agencies have historically relied upon. Following the implementation of EO 13636, which created the CSF with a focus on critical infrastructure organizations, it has been encouraging to see that the current administration required agency use of the CSF with EO 13800.

Agencies are clearly adapting to the risk-management approach and incorporating it into agency practices. However, risk management as an approach must permeate beyond the IT departments and must have buy-in more broadly among other parts of Government in order for the CSF to have the desired impact.

In particular, the inspector generals (IGs) must begin to understand how to audit properly to a risk-based approach. Too often the IGs seem to want to return to the checklist of cybersecurity controls. Under a risk-based approach like those encouraged under the CSF, an auditor must not only make a determination if the organization is implementing controls, but if the organization is prioritizing the implementation of controls properly.

To be fair, measuring a risk-based approach to cybersecurity management is more challenging than simply running through a list of things to determine whether they are being done or not. However, we should not allow that challenge to deter progress. Risk-based management is a well-understood approach, and is used extensively by the most sophisticated organizations in both the public and private sectors, with demonstrable results.