April 20, 2016

Federal Cybersecurity Detection, Response, and Mitigation

United States House of Representatives, Committee on Oversight and Government Reform, Subcommittee on Information Technology

One Hundred Fourteenth Congress, Second Session

Hearing Contents:

William Hurd
Subcommittee Chairman, Subcommittee on Information Technology
[View pdf]

Sanjeev Bhagowalia
Deputy Assistant Secretary for Information Systems & Chief Information Officer, Department of Treasury
[View pdf]

Steven C. Taylor
Chief Information Officer, Department of State
[View pdf]

Andy Ozment
Assistant Secretary for Cybersecurity and Communications, Department of Homeland Security
[View pdf]

Charles Carmakal
Vice President, Mandiant Consulting

Available Webcast(s):*

[Watch Full Hearing]

Compiled From:

- https://oversight.house.gov/hearing/federal-cybersecurity-detection-response-and-mitigation/

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Rep. Will Hurd Opening Statement

Subcommittee on Information Technology
Federal Cybersecurity Detection, Response, & Mitigation
April 20, 2016

Good morning, everyone.

Every day, federal agencies face a barrage of attacks on their information systems from a number of different actors. Attacks on both the public and private sectors consistently reveal one common truth – no one is immune.

In December of last year, Juniper Networks announced that malicious code had been placed in its ScreenOS software, leaving a gaping vulnerability in one of its legacy products.

This particular vulnerability may have allowed outside actors to monitor network traffic, potentially decrypt information, and even take control of firewalls. Within a matter of days, the company provided its clients—which include various U.S. intelligence entities and at least twelve federal agencies—with an "emergency security patch."

DHS and other law enforcement agencies acted swiftly to notify federal agencies of the breach and Juniper's security advisory. Both of their actions may have averted a potentially devastating breach of sensitive data. This is just one sophisticated example of the attacks that U.S. companies and their federal clients face on a daily basis.

In January of this year, the Committee sent letters to the heads of 24 federal agencies requesting an inventory of systems running the aforementioned software. Additionally, the Committee asked for an update on their progress in installing the corresponding security patch.

Of the twelve agencies affected, three, including the Department of Treasury, took longer than fifty days to fully install patches and mitigate the threat posed by this vulnerability.

This is absolutely unacceptable.

The inability of federal agencies to maintain a comprehensive view and inventory of their information systems and respond to Congress in a timely manner cannot be the status quo.

Last December, Congress passed landmark information sharing legislation, the Cybersecurity Act of 2015, which creates a voluntary cybersecurity information sharing process to encourage public and private sector entities to collaborate and share information. Moreover, the bill established the Department of Homeland Security as the sole portal for companies to share information with the federal government.

With their newly codified role, I look forward to working with Dr. Ozment and DHS on how to strengthen their own posture and ensure that they possess the necessary technical tools to detect and mitigate threats and disseminate threat information within the federal government.

Only by fostering this framework where government and private entities are able to freely share knowledge of security vulnerabilities, threat indicators, and signatures can we be sure that our network defenses are getting the best intelligence available.

In addition, we must continue to learn from the private sector. Industry leaders like ThreatConnect and FireEye are constantly pushing the envelope in what is possible in cybersecurity. The government should not seek to compete with them, but rather should harness these engines of innovation, learn from them, and safely cooperate with them under the guidance of good sense and personal liberty.

I hope that this hearing will serve as the starting line for a larger conversation on attribution. Various international groups and state-sponsored actors are constantly attempting to steal military secrets and expose the personally identifiable information of American citizens, and we cannot stand idly by while this happens. I believe that attribution is a form of deterrence.

This hearing presents an opportunity to learn how federal agencies can improve their overall cybersecurity postures, share more timely and relevant information, and work with the private sector in a way that benefits all involved, while respecting the institutions of commerce and privacy.

I welcome our witnesses and look forward to hearing your testimony today.

Written Testimony of
Sanjeev "Sonny" Bhagowalia
Deputy Assistant Secretary for Information Systems and Chief Information Officer
United States Department of the Treasury
Before the Subcommittee on
Information Technology of the
Committee on Oversight and Government Reform
United States House of Representatives

Introduction

Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, thank you for the opportunity to testify today on the Department of the Treasury's procedures and approach to the detection, response, and mitigation of cybersecurity vulnerabilities.

Cybersecurity is one of the top priorities at the Treasury, not only for the Office of the Chief Information Officer (OCIO), but also for our senior leadership at both the department and bureau levels. Like others in the public and private sectors, Treasury relies on technology to meet our mission of serving the American taxpayers and acting as a steward of the national economy. Trillions of dollars and millions of records are stored and processed using Treasury IT systems. We devote a great deal of time, effort, and resources towards securing those systems in order to successfully execute our mission and maintain the trust of the American public.

Our adversaries in the cyber realm make this an increasingly difficult task, but one at which we must continue to succeed. Those targeting our people and our systems continue to grow in their sophistication, resources, and determination. According to a GAO official, cybersecurity incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT) by all federal agencies increased more than 1,000 percent between 2006 and 2014.[1] Treasury's incidents have grown by a far smaller percentage over that same time period. However, Treasury is observing what the rest of U.S. industry and U.S. government has observed: cyber activity by our adversaries is growing in sophistication, volume, brazenness, frequency and potential impact. For example, each year we monitor hundreds of millions access attempts and millions of potentially malicious cyber events. In response to this ever-changing threat, we must continue to be vigilant against the *next* incident, not just the last one. We have improved our cybersecurity posture through a holistic approach of people, process (including policy and governance) and technology. We have also increased our spending on cybersecurity in the past few years to reflect the seriousness of the threat. Our Cyber Enhancement Account in the FY 2017 President's Budget reflects our ongoing commitment to transparency and judicious use of resources as we augment Treasury's cyber defenses. We are continuously and incrementally improving in management and oversight of our IT environment including cybersecurity. We are leveraging synergy opportunities across the enterprise through legal authorities (e.g., FITARA, FISMA, and the Clinger-Cohen Act) to more effectively use our people, processes, technology in the cyberspace.

[1] *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*, 7 (2015) (testimony of Gregory C. Wilshusen, Director, Information Security Issues).

Detecting and mitigating vulnerabilities in our environment before they are exploited by our adversaries is an essential component of Treasury's "defense-in-depth" strategy. Having the tools and processes to identify and close these potential holes, and the communication lines to spread the message across government and to our private sector partners, are the keys to effective threat mitigation.

I have divided my testimony into two parts, to answer the two questions posed by the subcommittee. The first part of my testimony will explain how we tackle this challenge at the Department of the Treasury. The second part of my testimony will outline how we participate in the government-wide federal cybersecurity community and support the lead agency for cybersecurity, the Department of Homeland Security (DHS).

I. Vulnerability Detection, Reporting, Response and Mitigation within Treasury

The Treasury Environment

As you know, the Department of the Treasury and its bureaus have widely varying missions requiring widely varying IT environments. Our department is a large, geographically and technically diverse enterprise. From the industrial focus of the U.S. Mint and Bureau of Engraving and Printing, to the massive data storage and analytics focus of the Internal Revenue Service, to the advanced economic modeling performed in the Departmental Offices, each Treasury bureau requires a different mix of technologies to accomplish the overall Treasury mission.

While Treasury bureaus are empowered to make the IT decisions necessary to execute their individual missions and carry out many of the operational security functions within their environments, the Treasury CIO is accountable to ensure that those decisions properly consider security implications and evaluate risk and vulnerabilities on an ongoing basis. To this end, Treasury has aligned our departmental cybersecurity strategy with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the OMB Cybersecurity National Action Plan (CNAP) to ensure a common understanding of our objectives across the enterprise. Treasury is fully supportive of the five-part NIST framework (identify, detect, protect, respond and recover) and is proceeding with a department-wide effort to implement all applicable portions of the CNAP. Vulnerability management is part of the NIST framework.

We follow the maxims that "cybersecurity is about risk management" and "if everything is a priority, nothing is a priority." Therefore, we must often make strategic decisions regarding where we should focus our efforts. To the extent possible, and especially in instances where time is of the essence, Treasury employs a risk-based approach to vulnerability remediation. Given the realities of a limited resource environment, Treasury and its bureaus start by remediating vulnerabilities on assets with the greatest risk exposure first, and move systematically to remediate the remaining assets. In addition to security risk, factors such as the operational risk posed to the business are evaluated during the remediation process. This prioritization enables bureaus to focus on fixing the most important vulnerabilities first while facilitating our ability to perform the mission of Treasury.

Vulnerability Detection

IT companies, government agencies, security researchers, and others identify thousands of security weaknesses each year in the devices and software that we all use on a daily basis. There are over 76,000 identified vulnerabilities in the National Vulnerability Database. In 2015 alone, over 6,000 new vulnerabilities were added to the database.[2] Critical vulnerabilities are a far smaller number and may represent weaknesses with respect to external or internal threats.

Vulnerability detection requires a multidimensional approach involving asset management, automated tools, monitoring of communication channels, and human analysis. Using each of the multidimensional approaches, Treasury identifies vulnerabilities in our environment that adversaries might exploit.

The foundation of good comprehensive vulnerability detection begins with understanding how the hardware and software is used throughout an organization through strong asset management. Employing this approach allows us to evaluate the impact of each new vulnerability announcement against the equipment in our environment. To this end, Treasury has policies in place requiring our bureaus to perform regular asset and vulnerability inventory scans using automated tools.

In addition to understanding the makeup of our IT environment and performing automated scans against known vulnerabilities, it is critical that we become aware of new vulnerabilities as quickly as possible after they are discovered. Treasury maintains a central security operations center (Treasury SOC) responsible for coordinated department-wide activity that operates around the clock working closely with bureau SOCs and security operations personnel to ensure protection of the department's IT assets. As one of its key functions, the Treasury SOC monitors classified and unclassified government channels, as well as open source and industry channels, for news of critical vulnerabilities and actively participates with other U.S. Government SOCs. Once critical vulnerabilities are identified, the Treasury SOC rapidly transmits the information to Treasury bureaus through alerting and notification channels. Bureau IT operations personnel assess the risk posed by the identified vulnerability to their respective networks and plan mitigation as appropriate, coordinating with the Department OCIO, who maintains overall oversight responsibility under FISMA and FITARA.

Additionally, the Treasury SOC and bureau security teams assess our collective ability to detect and block malicious activity targeting a given vulnerability. Whenever possible, new signatures or indicators are added to Treasury's defensive measures to mitigate risk or respond to any negative impact that may have occurred while the vulnerability was exposed.

Treasury also takes steps at both the enterprise and bureau levels to identify vulnerabilities that our automated scanning may not discover. Some of these countermeasures include penetration testing to uncover configuration or software and hardware vulnerabilities that hackers could exploit, as well as analyzing the attempts against us to identify patterns that may indicate a "zero-day," or undiscovered, vulnerability.

[2] https://nvd.nist.gov/

Response, Reporting, and Mitigation of Known Vulnerabilities

To keep up with the thousands of vulnerabilities and associated patches that are released and may apply to their respective environments, the initial response by bureau IT organizations is to undertake a risk analysis for each new vulnerability. Informed by the risk analysis, bureau IT organizations schedule testing and patch deployment as appropriate. This risk analysis aligns with best practices and typically is highly technical and detailed. Factors that bureau IT organizations may consider include the version and current patch levels of vulnerable software running on our hardware, as well as whether the software is configured to block the use of exploitable services and whether other defenses are in place or can be instituted to reduce the likelihood of an exploitable vulnerability. These security concerns are then balanced with operational assessments and testing to mitigate potential business impact that could result from deploying any patches.

A risk analysis may result in several mitigation approaches, such as patching, instituting compensating security controls, or migrating to a new software or hardware solution. These mitigation techniques are then evaluated through follow-on efforts. Compensating security controls may be assessed by a security professional, or automated tools used to scan and assess whether or not patches have been successfully applied throughout the department. This risk analysis and mitigation process covers the vast majority of patching and remediation efforts, and each Treasury bureau manages the timing and nature of the mitigation based on their established risk thresholds.

Bureaus are required to report a set of metrics on vulnerability assessment and remediation to OCIO on a monthly basis, including statistics on percent of assets scanned for known vulnerabilities, and statistics on patch implementation. Additionally, for certain highly important or highly critical vulnerabilities as determined by a risk analysis at the Treasury OCIO, remediation progress is tracked closely by OCIO.

The recent Juniper vulnerability offers an example of this process in action. Within a couple of hours after the vulnerability was announced by the equipment manufacturer, the Treasury SOC alerted bureau-level SOC counterparts to the vulnerability and to the mitigation instructions provided by the vendor. Additional updates and details from DHS were also transmitted to bureaus as they were received. Thanks to the quick action of the Treasury SOC and the bureaus' SOCs, remediation was already under way by the time government-wide alerts to patch vulnerable appliances were issued. Throughout the process, the Treasury SOC and OCIO gathered regular updates on remediation efforts via data call, which were communicated to DHS and Treasury leadership until the vulnerability was fully patched. For any highly critical vulnerabilities, the Treasury SOC and OCIO continue to monitor the remediation status until all the vulnerable assets are patched.

Some notable milestones in this mitigation effort across Treasury include:

- Treasury coordinated an enterprise-wide response to the Juniper vulnerability and patch within a couple of hours of receiving the information from open source vendor channels and DHS;

- Treasury fixed 25% of the patches in a day; 84% within a week; 86% within two weeks; and 93% in seven weeks;
- After a detailed analysis determined that two bureaus configurations posed low risk for exploitation of the vulnerability (because infected devices were not connected to the Internet and thus were not directly affected by the vulnerability and each had multiple compensating controls in-place) Treasury completed the remaining 7% of patching in just over eight weeks;
- DHS NCCIC submitted a notice to all agencies in the U.S. Government indicating close-out of the action on February 17, 2016;
- Treasury submitted the official status of the program to Congress on March 4, 2016.

Table 1 accompanying this testimony illustrates the timeline followed by Treasury in mitigating the vulnerability.

All organizations, both in the public and private sectors, face the same challenge in defending against the asymmetric nature of cyber incidents. To guarantee successful defense of our systems, we must be perfect 100 percent of the time; to penetrate our defenses, while our adversaries only need to succeed once. Federal government organizations face additional challenges working within the restrictions of a two-year budget cycle, compliance with a long list of regulations to defend against adversaries who may change tactics at Internet speed with a singular focus. It is noteworthy that many breaches outside Treasury have exacerbated our cyber efforts, as they have for many agencies across Government.

II. Treasury's Role in Government-Wide Vulnerability Detection, Response and Mitigation

Participation in Government-wide Vulnerability Mitigation

First, I would like to start by thanking DHS for their leadership role in federal government cybersecurity. As a member of the federal cybersecurity community, Treasury does its part to support the efforts of DHS and others to identify and remediate critical vulnerabilities. Treasury is an active participant in information sharing efforts, including the Automated Indicator Sharing program, the Cyber Response Group (CRG), and the Cybersecurity Coordination, Assessment, and Response (C-CAR) program. While programs such as C-CAR are instrumental in providing notifications regarding critical vulnerabilities across government, the speed at which our adversaries can identify and exploit vulnerabilities in our infrastructure makes rapid alerts all the more essential. Treasury also has a vast network across government and industry to share cybersecurity practices and lessons learned. Treasury has also engaged with DHS for penetration testing, Remote Vulnerability Assessments (RVA) for high value assets; exchanges information with the law enforcement and intelligence communities for threat awareness; fully participates in the DHS EINSTEIN program and looks forward to participating in the EINSTEIN 3A program; and uses world-class cyber organizations to independently assess our cyber posture.

Another challenge faced by large agencies in complying with government-wide mandates to address particular vulnerabilities is the need to balance operational and security risk. In many cases the devices that must be patched are part of complex systems with several legacy components that may not be compatible with a given security fix. If other security measures can mitigate risk while a patch is tested for interoperability with a particular system, that factor should be considered in reporting. As much as feasible, government-wide reporting on remediation compliance should factor in risk mitigation as well as raw patching numbers.

I would also like to share a success story of government working together to collectively improve our cybersecurity. In May 2015, DHS issued Binding Operational Directive 15-01, to mitigate the most critical vulnerabilities currently identified on Internet-accessible systems for all Federal Civilian Executive Branch Departments and Agencies. They detected 363 initial active critical vulnerabilities (external) across the Federal Civilian Executive Branch and Departments and Agencies reduced this initial set to two; a 99% reduction. Treasury fully participated in that initiative, reducing to and maintaining our number at zero.

Continuous Diagnostics and Mitigation (CDM) at Treasury

The Continuous Diagnostics and Mitigation (CDM) program led by DHS will help move Treasury and other departments and agencies from federated compliance to integrated continuous monitoring by implementing new technologies in three phases. Phase 1, which is currently being implemented at Treasury, will focus on managing our assets and identifying and prioritizing their vulnerabilities. Treasury is an enthusiastic participant in the CDM Program. Later phases will focus on managing our users and managing security events.

Treasury expects that CDM will lead to improved situational awareness regarding vulnerabilities in our environment. When a new vulnerability is discovered, Treasury will have a single data repository containing near real-time information about our entire asset inventory to analyze in order to more quickly assess our risk exposure. CDM will also enable better automation of vulnerability mitigation tracking in near real-time, reducing or eliminating in some cases the need for manual reporting of patch deployment through data calls. This will allow our staff to focus on assessing risk and remediating vulnerabilities rather than just reporting on them.

Conclusion

While Treasury has established a solid procedural and operational foundation to identify and mitigate vulnerabilities, our adversaries are constantly changing their methods, and we must remain vigilant to stop them. Continued collaboration with DHS, OMB, and the Congress on improved and streamlined notification as well as standardized toolsets through CDM will enable Treasury to more quickly learn of new vulnerabilities, as well as identify and remediate the affected aspects of our infrastructure.

Treasury understands that better use of our existing resources and strategic deployment of resources are just as important as new funding. Successful implementation of the Federal Information Technology Acquisition Reform Act (FITARA) provides opportunities for improvement in cybersecurity. FITARA can help to reduce the variance in IT asset profiles deployed across the agency, leading to faster mitigation of known vulnerabilities on common platforms. FITARA also enables us to better understand cybersecurity spending across the organization and identify opportunities for efficiency, allowing us to be better stewards of the public funds we already have rather than requesting additional support. Treasury secured full approval of our FITARA plan in December 2015 and will be reporting significant strides in our April report, thanks to on-going comprehensive reviews of major programs (including cyber).

Protecting against cyber intrusions remains a rapidly evolving challenge. In addition to the challenges and plans I already discussed, I see opportunities where Congressional support could aid our efforts:

1. First, hiring and retaining cyber security staff remains a challenge. We ask for continued support to streamline hiring and offer appropriate incentives to attract and retain that talent.
2. Finally, we ask for your consideration of our FY 2017 budget request for a Cybersecurity Enhancement Account, which will enable us to keep pace with the rapidly evolving adversaries through targeted and accountable spending.

Thank you for your attention to the important subject of vulnerability identification and remediation. I appreciate this opportunity to testify today and I will be glad to answer any questions you may have.

Table 1: Juniper Vulnerability Remediation Timeline

	Date						
	17-Dec	18-Dec	23-Dec	15-Jan	4-Feb	14-Feb	17-Feb
Days Elapsed From Announcement	Juniper and DHS Announces Vulnerability	1	6	29	47	59	DHS/NCCIC Issues Event Close-Out
High-Risk Devices Patched		14	40	40	40	40	
Low-Risk Devices Patched		0	8	11	13	17	
Total Patched		14	48	51	53	**57**	
% Complete		24.56%	84.21%	89.47%	92.98%	**100.00%**	

DEPARTMENT OF STATE

Testimony of Steven C. Taylor
Chief Information Officer
Bureau of Information Resource Management
before the
House Committee on Oversight and Government Reform
Subcommittee on Information Technology
United States House of Representatives
April 20, 2016

Chairman Hurd, Ranking Member Kelly, and distinguished members -- thank you for inviting me to testify about the Department of State's cyber security program.

THE THREAT

The Department of State, as the lead U.S. foreign affairs agency, has over 70,000 employees at our 275 overseas locations and at over 30 domestic locations.

Like all government agencies and businesses, particularly organizations the size of the Department, we face a dilemma. The Department uses the Internet and email to conduct our day-to-day operations, communicating with U.S. and foreign citizens and organizations about a wide variety of issues. We use these tools to support passport and visa applications, to communicate about key foreign policy initiatives, and to conduct the day-in, day-out business processes of the Department. We also know that email and the Internet are avenues through which our networks and databases can be attacked. As the breach of our own unclassified e-mail system in 2014 demonstrated, our adversaries see information handled by the Department – and many other U.S. government departments and agencies – as a desirable target. We experience millions of attempts to breach our networks and gain possession of our information annually. Protecting our information as we face increasingly sophisticated, frequent, and well-organized cyberattacks is one of the Department's top priorities.

THE DEFENSE

At the Department of State, the Bureaus of Information Resource Management and Diplomatic Security share the role of defending our networks through our joint security operations center and collaborative long-range planning. Working with the Department's Bureau of Diplomatic Security and alongside our partner federal agencies, we have developed increasingly robust defenses as the sophistication and intensity of these threats increase. The foundation of our cyber security framework is the Federal Information Security Modernization Act, along with OMB guidance and National Institute for Standards and Technology standards and guidelines, but we go far beyond those guidelines to protect our network and data while protecting the privacy and civil liberties of system users. The Department of Homeland Security (DHS) serves as a line of defense by filtering all our traffic through the Einstein system, which detects and blocks cyberattacks on federal civilian agencies, and through the Trusted Internet Connections initiative. In addition, we internally monitor with our own defensive toolset and capabilities. We also make great efforts to educate network users so they themselves defend our systems. Department of State network users must complete cyber security and privacy awareness training. In addition, network users are expected to answer a security challenge question prior to logging on to their system each day.

PARTNERSHIPS

We amplify the effectiveness of our defenses through partnerships with US-CERT, DHS, the Federal Bureau of Investigation, the National Security Agency (NSA), U.S. Digital Services, other agencies, and the private sector. DHS enhances our efforts through its Continuous Diagnostics and Mitigation program. Our partners in Diplomatic Security, intelligence community, DHS, other agencies, and the private sector perform penetration testing to ensure our defenses are capable of withstanding persistent attacks. Our partners provide us with a steady stream of information about probable sources and methods of attack, and recommend counter-measures.

MITIGATION

We recognize that intrusion is possible even with the best defenses. Today, we train and prepare for a wide range of cyber threats . Some can be contained by removing a hard drive, while others may require that we take systems off-line. We are constantly defending against known threats, and we work with our partners to protect against developing threats.

THE FUTURE

Looking to the future, the most powerful and promising tools for our defense are effective and efficient risk management, our public and private partnerships, clearly defined agency roles, effective information sharing, continuous education and reminders to our employees, and next generation technology. We appreciate the support of Congress on cybersecurity issues, and we look forward to working with Congress and our partners to defend our critical information and systems.

I would be happy to take any questions you may have.

Steven C. Taylor
United States Department of State
Bureau of Information Resource Management
Chief Information Officer

Steven C. Taylor, a member of the Senior Foreign Service with the rank of Minister Counselor, was appointed as the Chief Information Officer (CIO) for the Department of State on April 3, 2013. As CIO, he is responsible for the Department's information resources and technology initiatives and provides core information, knowledge management, and technology (IT) services to the Department of State and its 260 overseas missions. He is directly responsible for the Information Resource Management (IRM) Bureau's budget of $560 million, and oversees State's total IT/ knowledge management budget of approximately $1.6 billion dollars.

Preceding his assignment as CIO, he was the Department's Deputy Chief Information Officer (DCIO) and Chief Technology Officer of Operations.

Mr. Taylor served in a number of prominent positions in the Department, including Minister Counselor for Management, Director of the Department's Worldwide Messaging Systems Office, SMART Program Director, and Counselor for Communication and Technology. Prior to his DCIO assignment, he served as Management Counselor in Cairo and Athens. His other overseas assignments include Baghdad, Berlin, Bonn, London, Moscow, and Rabat.

Mr. Taylor joined the Foreign Service in 1988. He holds a Masters degree in Management Information Systems, and earned his undergraduate degree in Business Management from Boston University.

Written Testimony

of

Dr. Andy Ozment

Assistant Secretary for Cybersecurity and Communications

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Information Technology

Regarding

Federal Cybersecurity Detection, Response, and Mitigation

Introduction

Chairman Hurd, Ranking Member Kelly, and Members of the Committee, thank you for the opportunity to appear before you today. Recent compromises of federal agencies clearly demonstrate the challenge facing the government in protecting critical information systems for essential operations and safeguarding our citizens' and employees' personal information against sophisticated, agile, and persistent threats. Addressing these threats is a shared responsibility. I will discuss the roles of the Department of Homeland Security (DHS) in protecting civilian federal departments and agencies from cybersecurity risks. I will then outline my Department's role in communicating significant cybersecurity vulnerabilities to federal civilian Executive Branch agencies, tracking remediation across government, and helping agencies mitigate vulnerabilities as required.

The Role of the Department of Homeland Security in Federal Cybersecurity

Within DHS, the National Protection and Programs Directorate (NPPD) has three sets of cybersecurity customers: federal civilian agencies, private sector companies, and State, local, tribal, and territorial (SLTT) governments. Department of Defense (DOD) and intelligence community (IC) networks are outside of NPPD's remit. The Office of Cybersecurity and Communications at NPPD is not a law enforcement agency or a member of the intelligence community. Its sole focus is on helping our customers improve their cybersecurity. This testimony focuses on NPPD's role in securing federal civilian Executive Branch departments and agencies.

Under current law, each agency is responsible for managing its own cybersecurity risk. NPPD assists agencies through four lines of interrelated effort. First, NPPD provides cybersecurity protections in certain cases where interagency services are effective and costefficient. This baseline is principally provided by the EINSTEIN program, which detects and blocks cyber-attacks outside of agency perimeters, and the Continuous Diagnostics and Mitigation (CDM) program, which provides tools for agencies to identify and prioritize vulnerabilities and other risk conditions within their networks. Second, NPPD measures and motivates agencies to implement best practices through risk assessments and targeted guidance. Third, NPPD serves as a hub for cybersecurity information sharing between government and the private sector, through automated means wherever possible. And fourth, NPPD provides incident response assistance to agencies victimized by a cyber-attack.

NPPD's Role in Vulnerability Detection, Response, and Mitigation

Information Sharing

NPPD serves a key role for the federal civilian executive branch in expediting the resolution of significant cybersecurity vulnerabilities. This role begins when we first learn of a new significant vulnerability. Upon doing so, either through a public announcement, our standing relationships with the cybersecurity vendor and research community, or our own activities, our first priority is to rapidly promulgate actionable information to our partners. For federal civilian agencies, our principal tools for this immediate dissemination are the Cybersecurity Coordination, Assessment, and Response (C-CAR) calls and alerts via standing portals. C-CAR calls allow DHS to quickly convey information to Chief Information Security Officers (CISOs) across the federal civilian government. While C-CAR calls are our frontline mechanism for rapidly transmitting critical cybersecurity information across the federal cybersecurity community, we leverage secure portals managed by our National Cybersecurity and Communications Integration Center (NCCIC) to disseminate more detailed information about a specific vulnerability.

In conveying information about a particular vulnerability to federal agencies, we include detailed mitigation instructions and available contextual information necessary to help our partners understand the significance of the vulnerability and the implications of forestalling expeditious remediation. Generally, dissemination of information about a vulnerability via a C-CAR call and the NCCIC portal is sufficient to raise awareness across the federal government and encourage agencies to rapidly implement necessary mitigations. The *Federal Information Security Modernization Act* of 2014 provided DHS with another tool to drive agency behavior: binding operational directives. These directives allow the Secretary of Homeland Security to require that agencies take certain actions in response to a known cybersecurity risk. For example, Secretary Johnson issued a binding operational directive in May 2015, requiring that all agencies mitigate critical vulnerabilities identified in their Internet-facing devices within 30 days of the vulnerability being identified to them by DHS. We conduct recurring scans to identify vulnerabilities in these devices, and we provide each agency with a weekly report listing their vulnerabilities and providing mitigation recommendations. These scans are a critical tool in motivating agencies to address vulnerabilities in their Internet-facing decisions, and the binding operational directive proved effective in focusing agency attention. But binding operational directives are generally most effective where we can independently measure agency compliance and thereby ensure accountability. As discussed further below, the deployment of CDM sensors across civilian federal agencies will provide significant data to support future binding operational directives.

Data Collection

After disseminating information about a significant vulnerability, DHS often collects information about government-wide remediation progress. This information is used for two purposes: to understand the prevalence of a particular vulnerability across government and to drive individual agencies to more quickly implement required mitigations. Currently, this data collection process is largely manual. DHS, typically in coordination with the Office of Management and Budget, disseminates a data call via a C-CAR call. Agencies then submit data to a central repository. This approach has several disadvantages: it relies upon agency self-attestation of their vulnerabilities and remediation progress, it imposes a time-consuming data entry requirement on each agency, and it depends on agencies to update their data regularly and accurately. The CDM program is fundamentally changing this paradigm. Through the CDM program, DHS provides federal civilian agencies with continuous automated diagnostics tools to detect vulnerabilities in near-real-time. CDM is divided into three phases:

- CDM Phase 1 identifies vulnerabilities on computers and software on agency networks. It can be summarized as telling operators "what is in your network."
- CDM Phase 2 will detect potentially malicious user behavior and ensure that users' authorized access does not exceed their assigned role in the organization. It can be summarized as telling operators "who is in your network."
- CDM Phase 3 will assess activity happening inside of agencies' networks to identify anomalies that may indicate a cybersecurity compromise. It can be summarized as telling operators "what is happening on your network."

We have provided CDM Phase 1 tools to 97% of the federal civilian government. Agencies are now deploying CDM Phase 1 tools on their networks. We will provide CDM Phase 2 to federal civilian agencies by the end of this fiscal year. Once widely deployed, CDM Phase 1 will lead to significant advances in vulnerability detection and mitigation for the federal civilian government. First, CDM sensors allow agencies to automatically and recurrently identify vulnerabilities in hardware and software on their networks. In turn, agencies will have a more accurate and timely understanding of vulnerability prevalence than they are able to achieve today. Second, CDM will allow us to shift from current manual methods for collecting vulnerability data to automated data feeds from each agency. Instead of asking each agency to manually submit a list with the instances of a particular vulnerability, we will be able to derive such a list nearly instantaneously from data provided by each agency to the federal dashboard hosted in the NCCIC. Third, CDM will provide us with the ability to assign each vulnerability a particular "risk score" that will represent its relative criticality. By increasing the risk scores for significant vulnerabilities, CDM will allow us to drive prioritized remediation activity across the federal civilian executive branch far faster than we can today.

Assist Agencies with Remediation

Agency capabilities to rapidly remediate identified vulnerabilities are often varied. We provide agencies with technical assistance and consultative services upon request to mitigate complex vulnerabilities and help agencies design more secure systems and assets. As discussed further below, the President's Fiscal Year (FY) 2017 Budget significantly expands our capacity to provide this valuable service to federal agencies.

Case Study

On December 17, 2015, a vendor released an out-of-band security advisory for an operating system running on certain routers and other network devices. This advisory was released after the vendor discovered unauthorized code that could allow an attacker to take control of certain devices and to decrypt secure connections. The same day, we held a C-CAR call with federal CISOs, including necessary mitigations. One day later, we sent a request to nearly 50 agencies requesting information on the impacted operating system and progress in mitigating the vulnerability. We then used our EINSTEIN system to check whether any adversaries had attempted to compromise federal civilian agencies using the identified vulnerability. We have not identified any such attempts. Most agencies rapidly mitigated all instances of the vulnerability on their network. We worked with a small number of agencies that identified technical challenges during remediation to help them address the vulnerability or implement compensating controls. This example illustrates that the current process is well-exercised but relies on manual processes. We are also still not satisfied with how long it takes to ensure that a vulnerability is fully patched across the government. CDM will allow a necessary transition to automation and timely data analysis, and thereby inform better oversight for the government writ large and better cybersecurity at each agency.

How Congress Can Help

The FY 2017 President's Budget funds several activities that will significantly enhance our ability to manage vulnerability detection and mitigation across the federal civilian executive branch. First, the Budget funds a further acceleration of CDM and a new CDM phase focused on securing high-value data on agency networks. Second, the Budget provides resources for additional personnel to help agencies remediate complex vulnerabilities or to design more secure systems. Finally, the Budget funds more proactive assessment teams that use the same techniques as malicious hackers, known as "red-teaming." These assessment teams detect vulnerabilities that the agencies themselves may have missed and determine how easily an adversary could compromise the agency's network.

As noted, NPPD also has a significant role in helping the private sector secure itself. Many companies take a holistic approach to assessing and mitigating risks from cyber attacks, physical sabotage, and natural disasters, all of which can all result in disruptions to their essential services. As our nation continues to face increasing and evolving cyber threats and other risks, the Department must likewise use an integrated approach in preparing for these threats. In a major step toward this unified approach, the Department proposed to transition NPPD to an operational component, the Cyber and Infrastructure Protection Agency. This transition would elevate cyber operations and provide more comprehensive, coordinated risk management support to our stakeholders that reflect the growing convergence of cyber and physical threats. As one of the current priorities of the Secretary, the Department submitted a plan to NPPD's authorizing and appropriating committees, calling for congressional support and action. The transition, if implemented, would improve the services provided to NPPD's stakeholders. Not only would the transition provide a more comprehensive approach to national level stakeholder engagement and relationship management, but stakeholders in the field would also have access to a unified catalog of services and tools that spans across all of NPPD. For example, the plan proposes to establish regional offices to better integrate field staff like Protective Security Advisors and Cyber Security Advisors, and support coordinated engagement with industry partners on cyber and physical vulnerability assessments, information sharing, incident response and other efforts.

We need to position ourselves to successfully address the realities of today's cyber environment and its impacts on critical infrastructure. The proposed structural changes at the headquarters and regional levels will enable NPPD to be more efficient and effectively deliver the important tools and resources to our critical infrastructure stakeholders that need them the most. NPPD is committed to ensuring that our partners understand how disruptions and attacks on infrastructure can impact homeland security, community resilience, and our economy, and have the tools to drive informed action to mitigate those risks.

Conclusion

Vulnerabilities will continue to be identified and our adversaries will continue to use these vulnerabilities in attempting to compromise federal agencies. The key to effective vulnerability management is communication, automation, and resources for remediation. We have developed the government-wide processes for effective communication of significant vulnerabilities. With the help of Congress, we will continue driving toward additional automation and deploy the resources required to support expedited remediation. But this must be a shared effort. DHS, our partner agencies, and Congress must join together to ensure that vulnerabilities are rapidly mitigated before sensitive information or essential government services are placed at risk.

Dr. Andy Ozment

Assistant Secretary
Office of Cybersecurity and Communications
National Protections and Programs Directorate
Department of Homeland Security

Dr. Andy Ozment has worked in cybersecurity for almost twenty years as an operator, programmer, policymaker, and executive. He is currently the Assistant Secretary for Cybersecurity and Communications at the Department of Homeland Security (DHS). In this role, Dr. Ozment is charged with protecting the government against cyber attacks and helping the private sector protect itself.

Dr. Ozment's office helps its private sector and government customers by responding to incidents, sharing information, developing and promulgating best practices, and increasing our nation's cybersecurity capacity. In leading this office, Dr. Ozment oversees a budget of more than $1 billion and leads a workforce of over 600 federal employees and several thousand support personnel.

At DHS, Dr. Ozment has led the U.S. government's response to dozens of incidents in the government and private sector. Among recent events, he led the team that was called in to find and remove the intruders at OPM and separately to respond to the cyber attack that turned off power to over 200,000 individuals in the Ukraine. His team built and operates the first government-wide intrusion prevention system and is working with federal agencies to deploy endpoint monitoring solutions across millions of government computers. By establishing policy with clear metrics and holding agencies accountable, Dr. Ozment has driven a measurable decrease in the cyber risk faced by government agencies.

Prior to joining DHS, Dr. Ozment served at the White House as the President's Senior Director for Cybersecurity where he led a team that developed national policy and coordinated federal cybersecurity efforts. He was responsible for the development and implementation of the President's Executive Order 13636 on Improving Critical Infrastructure Cybersecurity. He then oversaw the resulting development of the NIST Cybersecurity Framework. Dr. Ozment also led the development of the National Strategy for Trusted Identities in Cyberspace, a signature initiative by the Administration to improve online authentication.

Prior to joining the White House, Dr. Ozment led an operational security group at DHS that oversaw compliance, metrics, and security authorization for the Department's Chief Information Security Officer. Previously, Dr. Ozment served in cybersecurity roles with the Office of the Secretary of Defense, National Security Agency, Merrill Lynch, and Nortel Networks.

Dr. Ozment earned a Bachelor of Science degree in Computer Science from Georgia Tech. While studying in the United Kingdom on a Marshall Scholarship, he earned a Master of Science degree in International Relations from the London School of Economics, and a Ph.D. in Computer Science from the University of Cambridge.