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 cost-

efficient. 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.