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 Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Regarding

DHS' Efforts to Secure .Gov

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and members of the Committee, thank you for the opportunity to appear before you today. Recent compromises clearly demonstrate the challenge facing the federal government in protecting 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 and in helping agencies better protect themselves.

The Role of the Department of Homeland Security in Federal Cybersecurity

The *Federal Information Security Modernization Act of 2014* specifies that federal agencies are responsible for their own cybersecurity. In addition, DHS has the mission to provide a common baseline of security across the civilian government and help agencies manage their cyber risk. DHS, through its National Protection and Programs Directorate (NPPD), assists agencies by providing this baseline for the federal government through the EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs, by measuring and motivating agencies to implement best practices, by serving as a hub for information sharing, and by providing incident response assistance when agencies suffer a cyber intrusion. I will discuss each of these in turn. NPPD has two additional cybersecurity customers besides the federal government: private sector infrastructure owners and operators, and State, local, tribal, and territorial governments. While several of the capabilities outlined below, such as information sharing and best practices, apply to all three customers, this statement focuses on NPPD's approach to federal cybersecurity in the context of the recent compromise at OPM.

EINSTEIN

EINSTEIN protects agencies' unclassified networks at the perimeter of each agency. Furthermore, EINSTEIN provides situational awareness across the government, as threats detected in one agency are shared with all others so they can take appropriate protective action. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

The first two versions of EINSTEIN – EINSTEIN 1 and 2 – identify abnormal network traffic patterns and detect known malicious traffic. This capability is fully deployed and screening all Federal civilian traffic that is routed through a Trusted Internet Connection (a secure gateway between each agency's internal network and the Internet). EINSTEIN 3 Accelerated (EINSTEIN 3A), which actively blocks known malicious traffic, is currently being deployed through the primary Internet Service Providers serving the Federal government. EINSTEIN 1 and 2 use only unclassified information, while EINSTEIN 3A uses classified information. Using classified indicators allows EINSTEIN 3A to detect and block many of the most significant cybersecurity threats. We are working aggressively to ensure that all agencies are protected by EINSTEIN 3A, including by implementing alternative deployment options that address the inability of some Internet Service Providers to implement EINSTEIN 3A in a sufficiently timely manner.

We are now accelerating our efforts and making significant progress in implementing EINSTEIN 3A across the federal government. The system now protects 15 federal civilian departments and agencies and over 930,000 federal personnel with at least one of its two security "countermeasures." Thus, EINSTEIN 3A protects approximately 45% of the civilian government - a 20% increase over the past 9 months alone. During this time, EINSTEIN 3A has blocked

nearly 550,000 attempts to access potentially malicious websites via one of its countermeasures. Any one of these blocked attempts could have conceivably resulted in an incident of severe consequence.

As we fully deploy EINSTEIN 3A, we are also mindful that to stay ahead of the adversary, we must go beyond the current approach that uses indicators of known threats. To that end, we are developing advanced malware and behavioral analysis capabilities that will automatically identify and separate suspicious traffic for further inspection, even if the precise indicator has not been seen before. We are examining best-in-class technologies from the private sector to evolve to this next stage of network defense. As I will discuss later, EINSTEIN played a key role in understanding the recent compromise at OPM.

Continuous Diagnostics and Mitigation (CDM)

Security cannot be achieved through only one type of tool. That is why security professionals that is why security professionals believe in defense-in-depth: employing multiple tools to, in combination, manage the risks of cyber attacks. EINSTEIN is a perimeter system, but it will never be able to block every threat. For example, it must be complemented with systems and tools inside agency networks.. Through the CDM program, DHS provides federal civilian agencies with tools to monitor agencies' internal networks. CDM is divided into three phases:

- CDM Phase 1 identifies vulnerabilities on computers and software on agency networks.
- CDM Phase 2 will monitor users on agencies' networks and detect if they are engaging in unauthorized activity.
- CDM Phase 3 will assess activity happening inside of agencies' networks to identify anomalies and alert security personnel.

We have provided CDM Phase 1 capabilities to 8 agencies, covering over 50% of the federal civilian government. We expect to purchase CDM for 97% of the federal civilian government by the end of this fiscal year. CDM will provide an invaluable tool in helping agencies protect against cybersecurity compromises. Although NPPD provides both EINSTEIN 3A and CDM capabilities to federal civilian agencies, each agency must still take action to implement these systems. In some cases, it may take agencies some months to fully implement a given capability once it is made available by DHS.

For example, a vignette from the current incident may be useful to illustrate how EINSTEIN and CDM jointly help protect federal agencies:

- As soon as OPM identified malicious activity on their network, they shared this information with DHS. NPPD then developed a signature for the particular threat, and used EINSTEIN 2 to look back in time for other compromises across the Federal civilian government. Through this process, we identified a potential compromise at another location with OPM data that would not have been identified and mitigated as quickly without the EINSTEIN system. We then used the EINSTEIN 1 system to determine whether data exfiltration had occurred.

- This same threat information is used by EINSTEIN 3A to block potential threats from impacting federal networks. Thus, DHS used EINSTEIN 3A to ensure that this cyber threat could not exploit other agencies protected by the system. As noted, DHS is accelerating EINSTEIN 3A deployment across the federal government. While it is challenging to estimate the potential impact of a prevented event, each of these malicious

DNS requests or emails that were blocked by EINSTEIN 3A may conceivably have led to a cybersecurity compromise of severe consequence.

- When implemented across the federal government, CDM will help agencies identify and prioritize vulnerabilities within their network. For example, CDM would have helped OPM identify any vulnerabilities within its database of federal personnel information and mitigate those vulnerabilities before they could be exploited by an adversary.

Measuring and Motivating Agencies to Adopt Best Practices

Many cybersecurity incidents can be avoided by simple measures. Implementing best practices is the foundation of cybersecurity. DHS works closely with individual agencies and governance bodies such as the Federal Chief Information Officer (CIO) Council to motivate agencies to implement best practices and to measure their progress in reaching particular goals and outcomes. Examples of best practices include patching critical vulnerabilities, implementing workforce training and awareness programs, and using multi-factor authentication. Secretary Johnson recently issued a Binding Operational Directive, based upon authority provided by Congress in the *Federal Information Security Modernization Act of 2014,* which directed civilian agencies to promptly patch vulnerabilities on their Internet-facing devices. These vulnerabilities are identified by recurring scans conducted by the DHS National Cybersecurity and Communications Integration Center (NCCIC). These vulnerabilities are accessible from the Internet, and thus present a significant risk if not quickly addressed. Agencies have responded quickly in implementing Secretary Johnson's directive, as over half of the stale critical vulnerabilities that existed when the Directive was issued have been mitigated within the 20 days since its issuance.

Under the authority provided by Congress in last year's FISMA legislation, DHS has a statutory role in developing, implementing, and evaluating operational cybersecurity guidance, in conjunction with the Office of Management and Budget. In this role, DHS leverages metrics, consultation, and strategic engagements with agency CIOs and Chief Information Security Officers (CISOs) to motivate agencies toward better cybersecurity. In fact, OPM was able to first identify the recent compromise of its network based upon technical recommendations provided by NPPD.

Information Sharing

Information sharing is an essential aspect of NPPD's cybersecurity role. By sharing information quickly and widely, we help other agencies block cyber threats before damaging incidents occur. Equally importantly, the information we receive from other agencies and the private sector help us understand emerging risks and develop effective protective measures. Our NCCIC is the civilian government's hub for cybersecurity information sharing, incident response, and coordination. In Fiscal Year 2015, the NCCIC has disseminated over 6,000 alerts, warnings, and bulletins.

To effectively combat sophisticated and agile adversaries, we must share information quickly enough to block threats before they can penetrate federal networks. We now have a system to automate our sharing of cyber threat indicators, and we are working aggressively to build this capability across government and to the private sector so we can share this information in near-real-time. One agency is already receiving cyber threat information via this automated system. We expect that multiple agencies and private sector partners will begin sharing and receiving information through this system by the end of October, 2015. As more agencies join

us in automated information sharing, we will increase our adversaries' cost and reduce the prevalence of damaging incidents across the federal government and the private sector.

Incident Response

Cybersecurity is about risk management, and we cannot eliminate all risk. Agencies that implement best practices and share information will increase the cost for adversaries and stop many threats. But ultimately, there exists no perfect cyber defense, and persistent adversaries will find ways to infiltrate networks in both government and the private sector. When an incident does occur, the NCCIC offers on-site assistance to find the adversary, drive them out, and restore service. In Fiscal Year 2015, the NCCIC has already provided onsite incident response to 32 incidents – nearly double the total in all of Fiscal Year 2014. The NCCIC also coordinate responses to significant incidents to give senior leaders a clear understanding of the situation and give operators the information they need to respond effectively. Similar to the recent incident at OPM, providing on-site incident response assistance also allows the NCCIC to identify indicators of compromise that can then be shared with other agencies and applied to EINSTEIN for broad protection across the federal government.

Cybersecurity Legislation

Last year, Congress acted in a bipartisan manner to pass critical cybersecurity legislation that enhanced the ability of the Department of Homeland Security to work with the private sector and other Federal civilian departments in each of their own cybersecurity activities, and enhanced the Department's cyber workforce authorities. As I noted, DHS is using the authority granted in one of those bills – the *Federal Information Security Modernization Act of 2014* – to

direct Federal civilian Executive branch agencies to fix critical vulnerabilities on their Internet-facing devices.

Additional legislation is needed. I previously highlighted EINSTEN's key role in identifying and mitigating an additional potential compromise during the OPM activity. The Department and Administration have a long-standing request of Congress to remove obstacles to the EINSTEIN program's deployment across Federal civilian agency information systems by codifying the program's authorities and resolving lingering concerns among certain agencies. Some agencies have questioned how deployment of EINSTEIN under DHS authority relates to their existing statutory restrictions on the use and disclosure of agency data. DHS and the Administration are seeking statutory changes to clarify this uncertainty and to ensure agencies understand that they can disclose their network traffic to DHS for narrowly tailored purposes to protect agency networks, while making clear that privacy protections for the data will remain in place. I look forward to working with Congress to further clarify DHS's authority to rapidly and efficiently deploy this protective technology.

In addition, carefully updating laws to facilitate cybersecurity information sharing within the private sector and between the private and government sectors is also essential to improving the Nation's cybersecurity. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of information shared without sacrificing the trust of the American people or the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be collated quickly in the NCCIC, analyzed, and shared quickly among trusted partners, including with law enforcement, so that network owners and operators can take necessary steps to block threats and avoid damage.

Conclusion

Federal agencies are a rich target and will continue to experience frequent attempted intrusions. This problem is not unique to the government – it is shared across a global cybersecurity community. The key to good cyber security is awareness and constant vigilance at machine speed. As our detection methods continue to improve, more events will come to light. The recent breach at OPM is emblematic of this trend, as OPM was able to detect the intrusion by implementing cybersecurity best practices recommended by DHS. As network defenders are able to see and thwart more events, we will inevitably identify more malicious activity and thwart the adversary's attempts to access sensitive information and systems. We are facing a major challenge in protecting our most sensitive information against sophisticated, well-resourced, and persistent adversaries. In response, we are accelerating deployment of the tools we have and are working to bring cutting-edge capabilities online. And we are asking our partner agencies and Congress to take action and work with us to strengthen the cybersecurity of our federal agencies.