Written Testimony

of

Dr. Andy Ozment

Assistant Secretary for Cybersecurity and Communications

U.S. Department of Homeland Security

Before the

U.S. Senate

Committee on Homeland Security and Government Affairs

Regarding

The OPM Compromise and the DHS Role in Federal Cybersecurity

Introduction

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for the opportunity to appear before you today. The Office of Personnel Management (OPM) compromise clearly demonstrates 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 Department's role in the recent compromise at OPM and how we are working with OPM and other agencies to accelerate improved cybersecurity across the Federal Government.

The Role of the Department of Homeland Security in Federal Cybersecurity

Cyber security, like physical security, requires layers of protections. The *Federal Information Security Modernization Act of 2014* specifies that federal agencies are responsible for their own cybersecurity. Although agencies must take the lead in their own cybersecurity, as OPM is currently doing, 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.

Like cameras, alarms, and fences around a physical building, 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. I am happy to discuss the Department's efforts to accelerate EINSTEIN 3A's deployment across the Federal civilian government, as well as the development of 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. EINSTEIN is a perimeter system, but it will never be able to block every threat. 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. I am happy to take any questions about how CDM protects networks and the role is play in cybersecurity, but first I want to address the current incident.

DHS's Role in the OPM Compromise

Breach of OPM Federal Personnel Records Stored by the Department of the Interior

Based on guidance provided by DHS in mitigating an earlier cybersecurity incident, the Office of Personnel Management (OPM) has spent the last year implementing improved cybersecurity capabilities across its networks. As a result, in April 2015, OPM became aware of a cybersecurity intrusion affecting one of its systems. As soon as OPM identified malicious activity on their network, they shared this information with the NCCIC. The NCCIC then used EINSTEIN 2 to look back in time for other compromises across the Federal civilian government. Through this process, the NCCIC identified a potential compromise at a Department of Interior data center which stored federal personnel records for OPM. Next, the NCCIC used the EINSTEIN 1 system to determine whether data exfiltration had occurred. In May, 2015, the NCCIC incident response team confirmed exfiltration of approximately 4.2 million federal personnel records stored at the DOI data center on behalf of OPM. NCCIC assesses that the adversary was present in the applicable DOI data center from October 2014 to March 2015.

Breach of OPM Background Investigation Records Stored by OPM Itself

In May 2015, as a result of continuing forensic analysis of its environment, OPM identified additional malicious activity on its own network. In June 2015, the inter-agency team determined that several OPM applications related to background investigations had been exposed to the adversary. NCCIC assesses that the adversary was present on OPM's network from June 2014 to January 2015. This remains an active investigation, and DHS, the FBI, and other partners are working closely with OPM to determine the extent of compromised background investigation information and potential implications. Information regarding this incident may change as the investigation progresses.

One of the important roles DHS plays is helping share information across agencies, and in some cases, with the private sector. For example, 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. 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.

DHS's Role in Federal Incident Reponses

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 coordinates 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 DHS's ability 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 through the recent issuance of a Binding Operational Directive.

Additional legislation is needed. I previously highlighted EINSTEIN'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 disappoint 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.