Testimony before the Committee on Oversight and Government Reform
U.S. House of Representatives

June 16, 2015

Sylvia Burns
Chief Information Officer
U.S. Department of the Interior

Good afternoon Chairman Chaffetz, Ranking Member Cummings, and distinguished members of the Committee. My name is Sylvia Burns and I currently serve as the Chief Information Officer (CIO) for the U.S. Department of the Interior (DOI). We appreciate the opportunity to testify regarding DOI's efforts to secure and protect agency, customer and employee data in the wake of the recently discovered cyber intrusion. Additionally, we appreciate having had the opportunity to provide a classified briefing on the cyber intrusion for members of your Committee staff, and other congressional staff, on May 21, 2015.

Cyber intruders executed very sophisticated tactics to obtain unauthorized access to Office of Personnel Management (OPM) data, hosted in a DOI data center, which contains sensitive personally identifiable information (PII). This incident was, and remains under active and ongoing investigation. At present, the investigation has not discovered evidence that any data, other than OPM data, was exfiltrated.

Concurrent with the ongoing investigation, DOI initiated a major planning effort to address short, medium and long-term remediation in order to strengthen our security protections and reduce risks to the Department, our employees, our customers and our partners. DOI takes the privacy and security of this data very seriously. We are working to support the current investigation regarding the incident affecting OPM data and to minimize the risk of future intrusions and their potential impact.

Background

In April, the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT) informed DOI about potential malicious activity, which was later determined to be an advanced persistent threat, on DOI's network.

As soon as DOI became aware of the suspicious activity, we began working with US-CERT, the Federal Bureau of Investigation (FBI) and other Federal agencies to initiate an investigation and determine what information may have been compromised. DOI allowed DHS and the other investigating agencies immediate access to the DOI's computer systems, and DOI dedicated staff to support the investigation.

Although, there is evidence that the adversary had access to the DOI data center's overall environment, today the investigation has not discovered evidence that any data, other than OPM data, was exfiltrated. It should be noted that DOI also performs shared services for other agencies. The investigation has not discovered evidence that any of its shared service customer data was exfiltrated. However, the investigation remains ongoing.

Remediation

Concurrent with the ongoing investigation, DOI immediately initiated a major planning effort to address short, medium and long-term remediation to strengthen our cybersecurity protections. We undertook those efforts in the context of other cybersecurity improvements, which were already underway pursuant to the Department's commitment to the Administration's cybersecurity cross agency priority (CAP) goals, as well as DHS's continuous diagnostics and mitigation (CDM) program. We have now accelerated our work on some of those activities, while also devising and implementing other security measures with the advice, guidance and consultation of investigating agencies with expertise related to this particular threat.

DOI is currently employing a comprehensive, multi-pronged remediation strategy to prevent, detect and act against malicious activity on our network in order to respond and recover following an incident. Central to this effort are measures to protect the data of our employees, customers and partners.

Activities that are underway include:

- We are working with DHS and our bureaus and offices to scan for malicious indicators across the entire DOI network.

- As part of DHS's Binding Operational Directive (BOD) we are identifying and mitigating critical Information Technology (IT) security vulnerabilities for all internet facing systems.

- The Secretary and Deputy Secretary expanded on DHS's BOD by directing my office – the Office of the Chief Information Officer (OCIO) – to take the lead in mitigating critical vulnerabilities for all of DOI's IT systems.

- We are acquiring and implementing new capabilities that will help us to detect and respond quickly to new intrusions. We continue to meet with interagency partners to learn about their activities and leverage that knowledge to continue to make additional improvements to our cyber security posture at DOI.

- We are fully enabling two factor authentication for privileged users (e.g., system administrators, etc.), as well as regular end-users.

DOI's existing long-term plans include several agency-wide strategic initiatives. For example, DOI is continuing its commitment to DHS's CDM program, which includes meeting our goal to complete the first round of activities around implementing hardware and software asset management. We are entering the second phase of DHS's CDM program activities. This will give DOI the ability to do application whitelisting, network access control to hardware, and dashboarding functionality to provide a comprehensive view of the Department's security posture.

Another important component of our long-term strategic plan includes strengthening DOI's cybersecurity and privacy workforce so that we have knowledgeable and experienced people to address current and future threats facing the agency. Having enough capable and dedicated cybersecurity, privacy and IT operations staff is critical to responding to threats and incidents, and sustaining normal operations following an intrusion.

Additionally, we are designing and implementing increased network segmentation so that, if an intrusion occurs within one component of our network, we can better limit the extent of the potential exposure. We are also evaluating data protection technologies such as information rights management for potential future investments. This will likely drive the modernization of legacy IT systems that cannot currently support data protections.

Conclusion

Again, DOI takes the privacy and security of its data very seriously. We are committed to supporting the continuing investigation regarding this incident affecting OPM data. Furthermore, we will continue to be an active participant in the ongoing efforts by the Federal government to improve our nation's overall cybersecurity posture.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my prepared statement. I would be happy to answer any questions that you may have.