Office of the Inspector General
United States Office of Personnel Management

Statement of
Michael R. Esser
Assistant Inspector General for Audits

before the

Committee on Oversight and Government Reform

United States House of Representatives

on

“OPM: Data Breach”

June 16, 2015

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Good morning. My name is Michael R. Esser. I am the Assistant Inspector General for Audits at the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today’s hearing on the information technology (IT) security audit work performed by the OPM Office of the Inspector General (OIG). Specifically, today I will be discussing the audits that our office has performed under the Federal Information Security Management Act, commonly known as “FISMA.” As I will describe, some of the issues identified in these audits date back to Fiscal Year (FY) 2007.

OIG’s FISMA Work

FISMA requires that OIGs perform annual audits of their agencies’ IT security programs and practices. These audits are conducted in accordance with guidance issued each year by the U.S.

Department of Homeland Security (DHS) Office of Cybersecurity and Communications. Today I will be discussing three of the most significant issues identified in our FY 2014 FISMA audit.

1. Information Security Governance

Information security governance is the management structure and processes that form the foundation of a successful information technology security program. Although the DHS FISMA reporting metrics do not directly address security governance, it is an overarching issue that impacts how the agency handles IT security and its ability to meet FISMA requirements, and therefore we have always addressed the matter in our annual FISMA audit reports.

In the FY 2007 FISMA report, we identified a material weakness[1] related to the lack of IT security policies and procedures. In FY 2009, we expanded the material weakness to include the lack of a centralized security management structure necessary to implement and enforce IT security policies. Although OPM's Office of the Chief Information Officer (OCIO) was responsible for the agency's overall technical infrastructure, each OPM program office had primary responsibility for managing its own IT systems. The program office personnel responsible for IT security frequently had no IT security background and were performing this function in addition to another full-time role. The agency had not clearly defined which elements of IT security were the responsibility of the program offices, and which were the responsibility of the OCIO.

As a result of this decentralized governance structure, many security controls went unimplemented and/or remained untested, and OPM routinely failed a variety of FISMA metrics year after year. Therefore, we continued to identify this security governance issue as a material weakness in all subsequent FISMA audits through FY 2013.

However, in FY 2014, we changed the classification of this issue to a significant deficiency, which is less serious than a material weakness. This change was prompted by important improvements that were the result of changes instituted in recent years. Specifically, in FY 2012, the OPM Director issued a memorandum mandating the centralization of IT security duties to a team of Information System Security Officers (ISSO) that report to the OCIO. In FY 2014, the OPM Director approved a plan to further restructure the OCIO that included funding for additional ISSO positions. The OCIO also established a 24/7 security operations center responsible for monitoring IT security events for the entire agency; however, OPM has not yet implemented a mature continuous monitoring program.

We have observed that this new governance structure has resulted in improvement in the consistency and quality of security practices for the various IT systems owned by the agency. Although we are optimistic that these improvements will continue, it is apparent that the OCIO continues to be negatively impacted by years of decentralized security governance. Although the IT security business processes are becoming more centralized under the CIO, the technical infrastructure remains fragmented and therefore inherently difficult to protect.

[1] An IT material weakness is a severe control deficiency that prohibits the organization from adequately protecting its data.

2. Security Assessment and Authorization

A Security Assessment and Authorization (Authorization) is a comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate in an agency's technical environment. The Office of Management and Budget (OMB) mandates that all Federal information systems have a valid Authorization.

OPM has a long history of issues related to system Authorizations. Our FY 2010 FISMA audit report contained a material weakness related to incomplete, inconsistent, and poor quality Authorization packages. This issue improved over the next two years, and was removed as an audit concern in FY 2012.

However, problems with OPM's system Authorizations have recently resurfaced. In FY 2014, 21 OPM systems were due for Authorization, but 11 of those were not completed on time and were therefore operating without a valid Authorization.[2] This is a drastic increase from prior years, and represents a systemic issue of inadequate planning by OPM program offices to assess and authorize the information systems that they own.

Although the majority of our FISMA audit work is performed towards the end of the fiscal year, it already appears that there will be a greater number of systems this year operating without a valid Authorization. The OCIO has temporarily put Authorization efforts on hold while it modernizes OPM's IT infrastructure in response to security breaches. We support the OCIO's effort to modernize its systems, but we believe that Authorization activity should continue, as the modernization is likely to be a long-term effort.

We believe that one of the core causes of these frequent delays in completing the Authorization packages is that there are currently no consequences for the owners of OPM IT systems that do not have a valid Authorization to operate. Although IT security responsibility is being centralized under the OCIO, it is still the responsibility of OPM program offices to facilitate and pay for the Authorization process for the IT systems that they own. Perhaps the most effective way to reduce delays would be to introduce administrative sanctions for non-compliance with FISMA requirements. We recommended that the performance standards of all OPM major system owners include a requirement related to FISMA compliance for the systems they own. Since OMB requires a valid Authorization for all Federal IT systems,[3] we also recommended that

[2] The OIG is the co-owner of one of these IT systems, along with OPM's Healthcare and Insurance (HI) and the Office of the Chief Financial Officer (OCFO), and the system is hosted by the OCIO. The system is the Audit Report and Receivables Tracking System, used to track the resolution of OIG audit recommendations, both procedural and monetary. The system does not collect or maintain any personally identifiable information. The OIG is working with HI, OCFO, and OCIO to resolve any issues.

[3] We acknowledge that OMB now allows agencies to make ongoing Authorization decisions for IT systems based on the continuous monitoring of security controls – rather than enforcing a static, three-year re-Authorization process. However, OPM has not yet developed a mature continuous monitoring program. Until such a program is in place, we continue to expect OPM to re-authorize all of its IT systems every three years.

the OPM Director consider shutting down systems that were in violation. None of the systems in violation were shut down.

Not only was a large volume (11 out of 47 systems) of OPM's IT systems operating without a valid Authorization, but several of these systems are among the most critical and sensitive applications owned by the agency.

Two of the OCIO systems without an Authorization are general support systems that host a variety of other major applications. Over 65 percent of all systems operated by OPM (not including contractor-operated systems) reside on one of these two support systems, and are therefore subject to any security risks that exist on the support systems.

Furthermore, two additional systems without Authorizations are owned by OPM's Federal Investigative Services, which is responsible for facilitating background investigations for suitability and security clearance determinations. Any weaknesses in the IT systems supporting this program office could potentially have national security implications.

Maintaining active Authorizations for all IT systems is a critical element of a Federal information security program, and failure to thoroughly assess and address a system's security weaknesses increases the risk of a security breach. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

3. Technical Security Controls

Our FY 2014 FISMA report contained a total of 29 audit recommendations, but two of the most critical areas in which OPM needs to improve its technical security controls relate to configuration management and authentication to IT systems using personal identity verification (PIV) credentials.

Configuration management refers to the policies, procedures, and technical controls used to ensure that IT systems are securely deployed.

OPM has implemented a variety of new controls and tools designed to strengthen the agency's technical infrastructure by ensuring that its network devices are configured securely. However, our FY 2014 FISMA audit determined that all of these tools are not being utilized to their fullest capacity. For example, we were told in an interview that OPM performs monthly vulnerability scans on all computer servers using its automated scanning tools. While we confirmed that OPM does indeed own these tools and that regular scan activity was occurring, our audit also determined that some of the scans were not working correctly because the tools did not have the proper credentials, and that some servers were not scanned at all.

OPM has also implemented a comprehensive security information and event management tool designed to automatically correlate potential security incidents by analyzing a variety of devices simultaneously. However, at the time of our FY 2014 FISMA report, this tool was receiving data from only 80 percent of OPM's major IT systems.

During this audit we also determined that OPM does not maintain an accurate centralized inventory of all servers and databases that reside within the network. Even if the tools I just referenced were being used appropriately, OPM cannot fully defend its network without a comprehensive list of assets that need to be protected and monitored.

This issue ties back to the centralized governance issue I discussed earlier. Each OPM program office historically managed its own inventory of devices supporting their respective information systems. Even though the OCIO is now responsible for all of OPM's IT systems, it still has significant work ahead in identifying all of the assets and data that it is tasked with protecting.

With respect to PIV authentication, OMB required all Federal IT systems to be upgraded to use PIV for multi-factor authentication by the beginning of FY 2012. In addition, OMB guidance also mandates that all new systems under development must be PIV-compliant prior to being made operational.

In FY 2012, the OCIO began an initiative to require PIV authentication to access the agency's network. As of the end of FY 2014, over 95 percent of OPM workstations required PIV authentication to access the OPM network. However, none of the agency's 47 major applications require PIV authentication. Full implementation of PIV authentication would go a long way in protecting an agency from security breaches, as an attacker would need to compromise more than a username and password to gain unauthorized access to a system. Consequently, we believe that PIV authentication for all systems should be a top priority for OPM.

Conclusion

As discussed above, OPM has a history of struggling to comply with FISMA requirements. Although some areas have improved, such as the centralization of IT security responsibility within the OCIO, other problems persist. Again, of particular concern is the high number of IT systems that are currently operating without a valid Authorization.

We acknowledge that OPM participates in multiple Government-wide security programs. However, these programs are designed to complement, not replace, a comprehensive IT security program. It is critical that OPM take steps to secure its network from within, and our audit recommendations are designed to help them do so.

Thank you for your time and I am happy to answer any questions you may have.