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 Appropriations

United States Senate

on

IT Spending and Data Security at OPM

June 23, 2015

Chairman Boozman, Ranking Member Coons, 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 discussing the information technology (IT) spending and data security at OPM. Specifically, today I will be discussing the audits that the Office of the Inspector General (OIG) conducts in accordance with the Federal Information Security Management Act, commonly known as "FISMA." Although OPM has made progress in certain areas, some of the current problems and weaknesses were identified as far back as Fiscal Year (FY) 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today.

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 talk about three of the most significant concerns highlighted in our FY 2014 FISMA report. However, it is important to note that our report contained a total of 29 recommendations covering a wide variety of IT security topics. Only 3 of these 29 recommendations have been closed to date, and 9 of the open recommendations are long-standing issues that were rolled-forward from prior year FISMA audits.

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.

This is an area where OPM has seen significant improvement. However, some of the past weaknesses still haunt the agency today.

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. OPM's Office of the Chief Information Officer (OCIO) was responsible for the agency's overall technical infrastructure and provided boundary-level security controls for the systems residing on this infrastructure. However, each OPM program office had primary responsibility for managing security controls specific to its own IT systems. There was often confusion and disagreement as to which controls were the responsibility of the OCIO, and which were the responsibility of the program offices.

Further, 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. For example, this meant that an employee whose job was processing retirement applications may have been given the additional responsibility of monitoring and managing the IT security needs of the system used to process those applications.

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.

---

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

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 by OPM. 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.

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, as the technical infrastructure remains fragmented and therefore inherently difficult to protect.

2. Security Assessment and Authorization

A Security Assessment and Authorization (Authorization) is a comprehensive process under which the IT security controls of an information system are thoroughly assessed against applicable security standards. After the assessment is complete, a formal Authorization memorandum is signed indicating that the system is cleared to operate in the agency's technical environment.

The Office of Management and Budget (OMB) mandates that all major Federal information systems have a valid Authorization (that is, that they have all been subjected to this *process*) every three years unless a mature continuous monitoring system is in place (which OPM does not yet have). Although, as mentioned, 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.

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.

[2] The OIG is the co-owner of one of these IT systems, the Audit Reports and Receivables Tracking System. This system has been reclassified as a minor system on the OPM general support system (GSS), and cannot be Authorized until the OCIO Authorizes the GSS.

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. In April, the CIO issued a memorandum that granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and for those scheduled to expire through September 2016. Should this moratorium on Authorizations continue, the agency will have up to 23 systems that have not been subject to a thorough security controls assessment. The justification for this action was that OPM is in the process of modernizing its IT infrastructure and once this modernization is complete, all systems would have to receive new Authorizations anyway.

While we support the OCIO's effort to modernize its systems, this action to extend Authorizations is contrary to OMB guidance, which specifically states that an "extended" or "interim" Authorization is not valid. Consequently, these systems are still operating without a current Authorization, as they have not been subject to the complete security assessment process that the Authorization memorandum is intended to represent.

There are currently no consequences for failure to meet FISMA standards, or operate systems without Authorizations, at either the agency level or the program office level. The OIG simply reports our findings in our annual FISMA audit, which is delivered to OPM and then posted on our website. OMB receives the results of all FISMA audits, and produces an annual report to Congress. There are no directives or laws that provide for penalties for agencies that fail to meet FISMA requirements.

However, at the program office level, OPM has the authority to institute administrative sanctions. This could be an effective way to reduce 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, we also recommended that 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.

As I explained, 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

As previously stated, 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 with OPM personnel 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 required 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.

Some of the other areas where we identified technical control weaknesses include:

- Operating system baseline configurations;
- Configuration change control;
- Tracking the status of known security vulnerabilities;
- Patch management;
- Termination of idle VPN connections, and;
- Continuous monitoring of security controls.

Finally, there has been much discussion of the problems with securing OPM's systems, as they are old, "legacy" systems. While this is true in many cases, and many of OPM's systems are mainframe-based, some systems that were impacted by the breaches are in fact more modern systems for which most of the technical improvements necessary to secure them could be accomplished.

<u>**OPM's Modernization Project**</u>

In April 2014, the agency began a full overhaul and modernization of its technical infrastructure, which will involve implementing additional IT security controls and then migrating the entire infrastructure to a completely new environment (referred to as the Shell). The OIG did not become aware of this project until nearly a year later, in March 2015, when we met with officials from the OPM's Office of the Chief Financial Officer and the OCIO to discuss questions related to the special $21 million funding request for this project contained in the President's FY 2016 Budget.

On June 17, 2015, we issued a Flash Audit Alert detailing concerns related to project management as well as the use of a sole source contract for the entire project. One specific issue discussed in the Flash Audit Alert was funding for the project.

OPM informed us that the current estimate for this project was approximately $93 million. However, after our auditors began their review, we learned that this cost estimate did not include the costs for migrating existing applications to the new Shell. That work is likely to be, by far, the most expensive part of the project. Migrating applications involves modifying all of the current systems – including all of the legacy systems that are frequently mentioned – so that they can operate in the new Shell environment. In 2009, OPM undertook a similar effort with its financial system application, and it cost $30 million and took two years. There are approximately 50 major systems that have to be migrated to the Shell, and many smaller ones.

Moreover, I am very concerned with the lack of an adequate funding plan for this project. Although there is a $21 million special request in the President's FY 2016 Budget, and DHS has committed $5 million to the Project, there is no comprehensive plan to fund the remaining costs of the project. Instead, we were told, in essence, that the OCFO would find the remaining funds somewhere, meaning a very heavy burden will fall upon program offices that are already stretched thin. The annual appropriations of program offices are meant to fund their core mission responsibilities, not subsidize a major agency-wide IT infrastructure project.

This last issue has also become significantly problematic for our own office. Because we were unaware that OPM had undertaken this immense project, we were unable to include the related costs in our FY 2016 budget request. The project will impose three types of costs upon us: (1) increased oversight costs, (2) the payment of the special assessment since we are a user of OPM IT services, and (3) the costs of modifying OIG-owned systems that reside on OPM's network so that they are compatible with the new IT environment.

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. Until OPM's security weaknesses are resolved, OPM systems will continue to be an inviting target for attackers.

If OPM's new modernization project is implemented appropriately, we believe that it will significantly improve OPM's IT operations, including its IT security posture. However, there are several issues, including significant budgetary concerns, which must be addressed. If they are not, we fear that there is a high risk this project will fail to meet its stated objectives.

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

United States Office of Personnel Management
1900 E Street NW, Washington, DC 20415

BIOGRAPHY

Michael R. Esser

Michael R. Esser was appointed Assistant Inspector General for Audits and to the Senior Executive Service in April 2006. Mr. Esser is responsible for overseeing the Office of Audits in conducting audits and special reviews of programs administered by the U.S. Office of Personnel Management, the largest of which are the Federal Employees Health Benefits Program (FEHBP), the Civil Service Retirement System and the Federal Employees Retirement System, and the Federal Investigative Services. His office also conducts audits of the Federal Employees' Group Life Insurance Program; Federal Employees Dental Vision Program; Flexible Spending Account Program; Federal Long Term Care Program; the agency's information systems, as well as information systems of the health carriers participating in the FEHBP.

Mr. Esser joined the Office of the Inspector General in February 1991 as an auditor, working primarily on the audits of the agency's consolidated financial statements. In November 2002, he was selected as the Chief of the Internal Audits Group, with responsibility for all audits of the agency's internal programs. Prior to coming to the U.S. Office of Personnel Management, Mr. Esser spent one year with a Northern Virginia CPA firm, and five years with Town & Country Mortgage Corporation in Fairfax, Virginia, the last three years of which was as Controller.

He attended George Mason University, graduating in 1984 with a Bachelor of Science degree in Accounting, and going on to earn a Masters in Business Administration in 1986. He is a member of the American Institute of Certified Public Accountants.