Office of the Inspector General
United States Office of Personnel Management

Statement of
Michael R. Esser
Assistant Inspector General for Audits

before the

Subcommittee on Research and Technology

and the

Subcommittee on Oversight

Committee on Science, Space, and Technology

United States House of Representatives

on

"Is the OPM Data Breach the Tip of the Iceberg?"

July 8, 2015

Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and Members of the Subcommittees:

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 to discuss our office's information technology (IT) security audit work, including our oversight of OPM's response to the recent data breaches and our annual audits required by 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 security breaches and loss of sensitive personal data at OPM.

OIG's FISMA Work

FISMA requires that Offices of Inspector General (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 IT 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.

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

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 by OPM. Specifically, in FY 2012, the then 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's continuous monitoring program cannot yet be classified as "mature" because the agency continues to rely on periodic ad hoc testing of security controls.

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 to Operate" (ATO) 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 be re-authorized 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.

There has been some discussion over the past few weeks regarding the importance of Authorizations. It is true that the ATO itself is simply a piece of paper and does not, in itself, indicate that a system is secure. Conversely, the lack of an ATO does not necessarily mean that a system is *not* secure. However, it is important to note that the intent of the ATO is to certify that a system was subject to the entire Authorization *process.* An agency IT system must be subjected to a thorough and independent assessment in order to determine whether the necessary security controls are in place and functioning appropriately. Without such an assessment, the agency will not know what weaknesses and vulnerabilities may be present. If the agency does not know what weaknesses and vulnerabilities exist in its IT environment, it cannot take steps to

address and remove those weaknesses, or develop a proactive and comprehensive IT security strategy.

OPM has a long history of issues related to system Authorizations, which we believe represents a long-standing pattern of neglect of IT security. 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. 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 ATO is intended to represent. We believe that this continuing disregard of the importance of the Authorization process is an indication that the agency has not historically, and still does not, prioritize IT security.

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. In addition, we recommended that the employee performance standards of all OPM major system

[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.

owners include a requirement related to FISMA compliance for the systems they own and it be included as part of their annual performance evaluation as a critical element. 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. Again, we acknowledge that the lack of an ATO does not, by definition, mean that a system is insecure. However, it absolutely does mean that a system is at a significantly higher risk of containing security vulnerabilities. The authorization process – nearly without exception – identifies significant issues that must be addressed. Considering the rapidly changing pace of technology, it is irresponsible to allow these systems to operate indefinitely without routinely subjecting them to a thorough security controls assessment.

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. 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:

- Baseline configurations: OPM has not documented pre-approved secure configurations for the operating systems it utilizes;
- Configuration change control: OPM cannot ensure that all changes made to information systems have been properly documented and approved;
- Patch management: Our vulnerability scan test work determined that numerous servers were not patched on a timely basis; and,
- VPN connections: VPN connections do not time out after 30 minutes of inactivity.

Modernizing OPM's IT Environment

OPM, like other Federal agencies, is facing the daunting, but not impossible, challenge of modernizing its IT environment.

In the past few weeks, there have been assertions that OPM's legacy information systems are supported by very old technology (specifically COBOL, a mainframe programming language), and therefore could not be protected by modern security controls. However, we know from our audit work that some of the OPM systems involved in the data breaches run on modern operating and database management systems. Consequently, modern security technology such as encryption or data loss prevention could have been implemented on these specific systems.

Also, OPM has stated that because the agency's IT environment is based on legacy technology, it is necessary to complete a full overhaul of the existing technical infrastructure in order to address the immediate security concerns. While we agree in principle that this is an ideal future goal for the agency's IT environment, there are steps that OPM can take (or has already taken) to secure its current IT environment.

For example, OPM has significantly upgraded security controls to protect the perimeter of its network. In addition, some of OPM's most sensitive systems are compatible with additional security controls such as data encryption and other data loss prevention techniques, which could be utilized to protect OPM's systems. Another step that OPM could take would be implementing full two-factor authentication to access OPM's major IT systems. This would add an additional layer of defense that will go a long way toward preventing additional data breaches.

A more in-depth process for improving the security of OPM's systems will involve a comprehensive analysis of their fundamental design. OPM recently disabled access to its Electronic Questionnaire for Investigations Processing system (referred to as e-QIP), which is used to collect information related to Federal background investigations, because of serious vulnerabilities detected in the design of the database and public-facing website.

OPM's official statement on this issue claims that the agency is acting proactively by shutting down the e-QIP system. However, the current security review ordered for this system is a direct reaction to the recent security breaches. In fact, the e-QIP system contains vulnerabilities that OPM knew about, but had failed to correct for years. As part of the system's Authorization process in September 2012, an independent assessor identified 18 security vulnerabilities that could have potentially led to a data breach. These vulnerabilities were scheduled to be remediated by September 2013, but still remain open and unaddressed today.

Unfortunately, the overdue remediation of known vulnerabilities for e-QIP is only a single example of a more widespread problem at OPM. Both our FY 2012 and FY 2013 FISMA reports indicated that out of OPM's 47 major information systems, 22 had known vulnerabilities with remediation activity greater than 120 days overdue. In FY 2014, the number grew to 38.

This issue demonstrates the importance of the Authorization process (as discussed above), but is also an example of OPM's historical neglect of IT security. The agency has failed to complete

system Authorizations for its most sensitive systems, but even when the agency has known about security vulnerabilities, it has failed to take action.

OPM's Infrastructure Improvement Project

In April 2014, in response to the March 2014 breach, OPM initiated a major IT overhaul (referred to as the Project). The initial plan was to make major security improvements to the existing environment and continue to operate OPM systems in their current location. During the process of implementing security upgrades, OPM determined that it would be more effective to completely overhaul the agency's IT infrastructure and architecture and move it into an entirely new environment (referred to as the Shell).

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. OPM provided a written response to our Flash Audit Alert on June 22, 2015. Below is a brief description of some of our specific concerns, as well as OPM's response.

- Missing planning documentation: As per OMB requirements, the agency must prepare a Major IT Business Case proposal (formerly known as an Exhibit 300) for a project of this size and scope. This document requires that the agency fully evaluate the costs, benefits, and risks associated with the Project. In response to our Flash Audit Alert, OPM officials stated that an overarching Major IT Business Case proposal is not necessary since they view the various phases of this project as extensions of existing IT investments established by previous Major IT Business Case proposals. OPM officials also objected to the amount of time required to complete such a proposal since it would negatively impact their implementation plans.

  We disagree with this view because this is a new project creating an entirely new IT infrastructure and architecture. Many of OPM's approximately 350 major and minor IT systems will need to be completely redesigned to be compatible with the new environment. This is clearly a major initiative that requires a Major IT Business Case proposal, especially to fund the migration effort. In addition, the process of creating the proposal, and the related artifacts that are generated during the effort, will serve as an invaluable project management tool throughout the life cycle of the Project.

- Best practices and requirements not followed: OPM officials have also failed to follow industry best practices as well as OPM's own System Development Life Cycle requirements for basic project management activities and documents. On July 1, 2015, OPM officials provided a status of their progress in preparing some of these items. Most of the activities and documents, which should have been completed prior to the Project's initiation, have still not been completed.

- Lack of a complete inventory: In order to determine the capabilities and functions that the new IT environment would have to perform, OPM first needs a complete list of all of the IT systems that will have to be housed on the new platform. OPM has a plan in place to develop such an inventory, but it is not yet complete.

- Lack of comprehensive cost estimate: OPM had estimated that the cost of the Project would be $93 million, but this estimate does *not* include the costs of migrating all of the agency's existing IT systems to the new Shell. This will be, by far, the most costly part of the Project. However, without a complete inventory of all of the IT systems that need to be migrated, OPM cannot develop a reliable cost estimate. To compare, when OPM had to migrate a single system (its financial system) to a new cloud-based environment, it took two years and approximately $30 million to complete. This Project is much larger, involving approximately 350 major and minor systems.

- No dedicated funding stream: Another related concern is that there is no dedicated funding stream for the entire Project, creating a very high risk that funding will be inadequate to support the complete migration effort. When combined with our serious concerns about the lack of a disciplined project management approach, the failure to identify a funding stream for the Project creates a high risk that the Project will fail to meet its stated objectives of creating a more secure IT environment at a lower cost.

- Use of a sole-source contract: Our review of procurement documents and discussions with senior OPM officials indicated that they plan to use a sole-source contract for the entire Project. We agree that the initial phase of the Project (immediately strengthening OPM's IT infrastructure in response to the March 2014 breach) was a quick response to an emergency, and thus use of a sole-source contract was appropriate. However, the later phases of the Project are not urgent and the contracts for those services should be subject to full and open competition. Moreover, it should be noted that the later phases of the Project, such as the migration of systems to the Shell, require a wide array of skill sets. It is highly unlikely that a single vendor could provide all of the necessary services for the migration effort.

  Although OPM has publicly stated that the sole-source contract was intended only for the first two phases of the Project, it was clearly indicated in the documents we reviewed, as well as during discussions with the OCIO, that the contract was intended to cover the entire Project. If OPM now plans to use full and open competition for the remainder of this effort, we welcome this new approach. We will continue to monitor the use of the sole-source contract to ensure that OPM complies with appropriate regulations.

We are currently working with OPM to obtain additional information regarding these issues. The OIG will continue to monitor the progress of this Project and communicate any concerns we may have, both in writing and in meetings with OPM officials. We hope that the agency will address the significant deficiencies we have identified because if they do not, we believe that the Project has a high risk of failure.

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.