Office of the Inspector General
United States Office of Personnel Management

Statement of the Honorable
Patrick E. McFarland
Inspector General

before the

Committee on Oversight and Government Reform

United States House of Representatives

on

"OPM Data Breach: Part II"

June 24, 2015

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

Good morning. My name is Patrick E. McFarland. I am the Inspector General of the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today's hearing.

Before I begin, I would like to clarify two points that were discussed before this Committee on Tuesday, June 16, 2015. First, there were several statements made 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 and prevent the type of attacks that occurred in 2014. 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 could be utilized to protect OPM's systems. Moreover, implementing full two-factor authentication to access OPM's major IT systems will add an additional layer of defense that will go a long way toward preventing additional data breaches.

Second, at the hearing last week it was also stated that all information systems that we identified as not having a current Authorization in the FY 2014 FISMA report have since been Authorized. I believe that the comments were in reference to a memorandum issued by the Chief Information Officer (CIO) in April 2015 that granted an extension of the previous Authorization for the 11 systems in question. However, in its annual Federal Information Security Management Act (FISMA) reporting guidance, the Office of Management and Budget (OMB) specifically states that an "extended" or "interim" Authorization is not valid; therefore, these systems are not in fact Authorized.[1]

In addition, the CIO's memorandum does not resolve the primary concern. The Authorization itself is a formal document that grants permission for an information system to operate in a production environment. The *process* of Authorization is the relevant issue, since it involves a comprehensive assessment of a system's security level, risks, and controls. The fact remains that this process has not been completed for the 11 systems identified in the Fiscal Year (FY) 2014 FISMA audit report.[2]

OPM's Infrastructure Overhaul Project

In April 2014, in response to the March 2014 breach, OPM initiated a major IT overhaul. 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

---

[1] 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.

[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.

IT infrastructure and architecture and move it into an entirely new environment (referred to as the Shell).

There are four phases in the Project:

- Tactical – shoring up the existing security environment
- Shell – creating the new data centers and IT architecture
- Migration – migrating all OPM systems to the new environment
- Clean-up – decommissioning existing hardware and systems

Our understanding is that the Tactical phase was completed in April 2015 and the Shell phase is underway and is expected to be completed this fall.

We support OPM's efforts to modernize and better secure its IT environment; however, we have two significant concerns with this Project, resulting in an issuance of a Flash Audit Alert.

Flash Audit Alert

The typical audit process can take up to 10 to 12 months from the start of the audit to the issuance of the final report. As part of our normal audit process, we provide a draft audit report to OPM for comment. It is a fact finding step to ensure that our audit field work is complete and accurate. We consider those comments, make any necessary changes, and incorporate them into our final audit report.

However, sometimes in the course of our work, we discover significant evidence of a critical problem that needs *immediate* attention by OPM. In those situations, we issue what is called a "Flash Audit Alert." We do not normally provide a draft of this alert to the agency for comment given the time sensitive nature of the matter.

After our auditors finished conducting their initial review of the Project, we determined (1) the situation was serious enough to issue a Flash Audit Alert and (2) because of the significance of the Project, we would provide the agency with a brief window to provide comments on the draft alert.

We provided a draft copy of our Flash Audit Alert to the Office of the Chief Information Officer (OCIO) on June 2, 2015, after verbally briefing the CIO several days before. We requested comments by June 5th, and later extended that to June 10th. By June 17th we still had not received comments, or indication that comments would be forthcoming. Because of the urgency of the situation, I issued the Flash Audit Alert without the benefit of agency comments.

The two primary concerns discussed in the Flash Audit Alert relate to (1) project management and (2) the use of a sole-source contract.

1. Project Management Activities

The most significant shortcoming of OPM's management of the Project is that it has not prepared a "Major IT Business Case" proposal (formerly known as the OMB Exhibit 300), as required by OMB for IT projects of this size and scope. Preparing an OMB proposal would require OPM to fully evaluate the costs, benefits, and risks associated with its planned Project, and present its business case to OMB to seek approval and funding.

OMB Circular A-11 Appendix 6 defines capital budgeting requirements for capital asset projects. The basic concepts are that capital asset projects require proper planning, cost/benefit analysis, financing, and risk management. This includes demonstrating that the return on investment exceeds the cost of funds used, and that the full cost of the project is appropriated before work begins. Finally, the Circular requires risk management and earned value management throughout the life-cycle of the Project to ensure that it continues to meet cost and schedule targets.

For OPM to complete this process it must first fully determine the true scope and cost of the project. However, we learned from our audit work that OPM is still evaluating its existing IT architecture, including the identification of all mainframe applications that will need to be migrated to the Shell environment. Further, other systems will need to be redesigned before they can be migrated. There are approximately 50 major IT systems in OPM's inventory, and a large number of related sub-systems. Until this evaluation is complete, OPM is not able to estimate how long it will take or how much it will cost to complete the Migration phase of the Project.

Despite this, OPM officials informed us that the Migration phase will be complete in 18 to 24 months. We believe that OPM is highly unlikely to meet this target. Many critical OPM applications (including those that process annuity payments for Federal retirees, reimburse health insurance companies for claims payments, and manage background investigations) run on OPM's mainframe computers. These applications are based on legacy technology, and will need to be completely renovated to be compatible with OPM's proposed new IT architecture.

This will be a highly complex and monumental task. OPM has a history of troubled system development projects. Despite multiple attempts OPM has failed to modernize its retirement claims processing system. Although the 2009 revamp of OPM's financial system (now called CBIS) was ultimately partially successful, it was also fraught with difficulty. The CBIS project was the main focus of agency leadership at that time. It was relatively well managed, and was subject to oversight from several independent entities, including my office, but it still required two years and over $30 million to complete.

OPM's current initiative will be far more complex than anything OPM has attempted in the past, since each individual application migration should be treated as its own project similar to these examples. Furthermore, there are many other systems besides OPM's mainframe applications that will also need to be modified to some extent to be compatible with the Shell environment.

Even more troubling is the fact that OPM has not followed basic best practices for program management including developing a project charter, a comprehensive list of stakeholders, a feasibility study and impact assessment, test plans, and other standard project management artifacts.

In addition to defining cost and schedule targets, the OMB Major IT Business Case process is intended to secure funding for major IT investments before work begins. However, OPM has already committed substantial funds toward this project without completing the process. In FY 2015 OPM has obligated approximately $32 million toward shoring up its existing IT security controls and establishing the Shell environment. In its FY 2016 budget request, OPM requested and received an additional $21 million from OMB for the Project.

OPM program officials told us that some of the Project's funding will come from the $21 million budget request, $5 million from the U.S. Department of Homeland Security, and from assessments on the program offices. In addition, program offices will be required to fund the migration of applications they own from their existing budgets. However, program office budgets are intended to fund OPM's core operations, not subsidize a major IT infrastructure project.

It is unlikely that OPM will be able to fund the substantial migration costs related to this Project without a significantly adverse impact on its mission unless it seeks dedicated funding through Congressional appropriation. Also, OPM's current budget approach seems to violate IT spending transparency principles promoted by OMB's budget guidance and its IT Dashboard initiative, which is intended to "shine [a] light onto the performance and spending of IT investments across the Federal Government."

Without a dedicated funding stream, there is a very high risk that funding will be inadequate to support the entire Migration phase, which is likely to be complex, time consuming, and extremely expensive. In addition, without the disciplined project management processes that are associated with the OMB Major IT Business Case process, there is a high risk that this Project will fail to meet all of its stated objectives. In this scenario, the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources, possibly making both environments less secure, and increasing costs to taxpayers. This outcome would be contrary to the stated goals of creating a more secure IT environment at a lower cost.

The best chance for a successful modernization of OPM's IT environment is to develop and execute a comprehensive plan based on accepted project management disciplined processes.

2. Sole-Source Contract

OPM has secured a sole-source contract with a vendor to manage the infrastructure improvement project from start to finish. Although OPM completed a Justification for Other Than Full and Open Competition (JOFOC) to justify this contract, we do not agree that it is appropriate to use this contract for the entire Project.

The initial phase of the Project covered the procurement, installation, and configuration of a variety of software tools designed to improve the IT security posture of the agency (the Tactical phase). We agree that recent security breaches at OPM warranted a thorough and immediate reaction to secure the existing environment, and that the JOFOC was appropriate for this activity. However, we do not agree that it is appropriate to use a sole-source contract for the long-term system development and migration efforts.

OPM officials informed us that the reason for using the sole-source contract for the long term was to ensure continuity. The OCIO believes the same vendor that helped build the infrastructure should be responsible for migrating applications into that environment.

Federal Acquisition Regulation § 6.302 outlines seven scenarios where contracting without full and open competition may be appropriate, two of which relate to an unusual and compelling urgency and national security implications. There is no exception to the requirement for full and open competition for vendor continuity for the convenience of the agency.

The current vendor may well be chosen as the successful bidder through full and open competition when the Migration and Clean-up phases begin. Without subjecting the remainder of this process to competition, there is a high risk that project costs will be inflated. Further, it is highly unlikely that any single vendor is qualified for the Migration phase. OPM's information systems are supported by a wide variety of operating systems, databases, and programming languages. Each individual application migration will likely require dedicated contractor support by a vendor that specializes in the specific technology supporting that system.

The Migration and Clean-up phases are not responses to a crisis situation, as the Tactical phase was. Therefore, we believe that OPM should subject the remainder of the project to contracting vehicles other than the sole-source contract used for the Tactical and Shell phases.

Conclusion

While I fully support OPM's efforts to modernize its IT environment, I am concerned that there is a high risk that its efforts will ultimately be unsuccessful. For example, if the Migration phase fails, the results could be catastrophic. The agency could end up with half of its systems in the new Shell environment and half of its systems in the legacy environment. Neither of the environments would be fully secure, and OPM would be in a position where it is forced to pay indefinitely for the overhead costs of both infrastructures.

System development projects by their very nature are complex and prone to failure. Even with the application of strict project management techniques, many projects either fail entirely, or are only partially successful. Even so, there is a chance that this effort will ultimately succeed given time, leadership, and strong project management.

I am happy to answer any questions you may have.