UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Office of the
Inspector General

May 18, 2016

MEMORANDUM FOR BETH F. COBERT
Acting Director

FROM: NORBERT E. VINT
Acting Inspector General

SUBJECT: Second Interim Status Report on the U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project – Major IT Business Case (Report No. 4A-CI-00-16-037)

Executive Summary

This interim status report discusses the events that have transpired since the Office of the Inspector General's (OIG) September 3, 2015 Interim Status Report, as they apply to the concerns outlined in the initial June 17, 2015, Flash Audit Alert – U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project. We submitted a draft copy of this report to Office of the Chief Information Officer (OCIO) representatives to elicit their comments on our findings, conclusions, and recommendations. The OCIO's comments on the draft report were considered in preparing the final report and are attached as an Appendix to this report.

OPM has still not performed many of the critical capital project planning practices required by the Office of Management and Budget (OMB). Of primary concern, prior to initiating the Infrastructure Improvement Project (Project), OPM did not perform the mandatory Analysis of Alternatives to evaluate whether moving all infrastructure and systems to a new environment (initially known as Shell, but now referred to as IaaS [Infrastructure as a Service]) was the best solution to address the stated objective of this initiative: to provide a secure operating environment for OPM systems at a lower cost. In light of recent developments involving the creation of the National Background Investigations Bureau within OPM to replace the Federal Investigative Services, the current Federal background investigations program, and the shifting of the responsibility for developing and maintaining the associated information technology systems to the Department of the Defense, this analysis is even more important. In addition, most, if not all, of the supporting project management activities required by OMB have still not been completed.

Furthermore, the estimated lifecycle costs of the Project are unsupported by any detailed technical analysis of the level of effort needed to modernize OPM systems and migrate them to the IaaS platform. However, OPM has made strides in identifying the inventory of its IT systems being moved to the new environment, and performing a risk analysis to determine the timing of modernization and migration activities.

The primary concern outlined in our June 2015 Flash Audit Alert was that OPM had not followed disciplined project management best practices in its effort to fully overhaul and migrate the agency's technical infrastructure to the IaaS. We recommended that OPM complete an OMB Major Information Technology (IT) Business Case (Business Case) that encompassed the full scope of this project, and explicitly stated that the use of project management practices should be associated with this process.

Although OPM initially disagreed with our recommendation, the agency ultimately submitted a Business Case to OMB as part of the fiscal year (FY) 2017 budget process and subsequently informed our office and the Congress that it now had a formal plan for this major initiative. However, we have reviewed the Business Case documentation and have concluded that the efforts put forth by OPM do not meet the OMB requirements and thus have not fully addressed the intent of our recommendation.

Major IT Business Case

A. Capital Planning Process

As reported in our June 2015 Flash Audit Alert, OPM initiated its Project without preparing a proper Business Case to seek approval and secure funding from OMB. OPM initially objected to our recommendation to do so, asserting that it would take too long and delay critical activities already in process.[1] On August 3, 2015 we were alerted that OPM had changed course, and now agreed to develop a Business Case that would be completed by September 30, 2015.

At the time it seemed unlikely that OPM would be able to complete the OMB-required capital planning process that would support such a document with the necessary level of rigor in this short timeframe. Our review of OPM's September 30, 2015 Business Case has

[1] "Completing and submitting an initial OMB Major IT Business Case document requires anywhere from eight months to a year of research, consultations, discussion, and effort." Memorandum to McFarland from Archuleta, *Response to Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project* (June 22, 2015), at page 2.

confirmed that OPM officials failed to perform almost all of the capital planning activities that are required to be associated with a Business Case document.

OMB Circular A-11 is the primary document that instructs agencies how to prepare and submit budget requests for OMB review and approval. The Capital Programming Guide is a supplement to this circular, and is intended to assist agencies to "effectively plan, procure, and use [capital] assets to achieve the maximum return on investment." Capital assets include IT hardware, software, and modifications.

Also, Section 5122 ("Capital Planning and Investment Control") of the Clinger-Cohen Act specifically requires that agencies establish a process for maximizing value and minimizing risk associated with IT acquisitions.

The process outlined in the Capital Programming Guide supplement to Circular A-11 involves the appointment of an integrated project team as the first step associated with major IT investments. Such a team should consist of experts from a variety of disciplines (including project management, procurement, cost estimating, risk management, budget, etc.) to manage the project throughout its lifecycle. One of the first activities that the integrated project team should carry out is an analysis of alternative courses of action.

This is referred to in OMB's budget guidance as the Analysis of Alternatives process. As part of this process, the integrated project team should consider a variety of factors, including availability of different options, affordability, cost and benefits, and risk. The team should conduct market research to identify as many alternatives as possible, develop a project baseline consisting of a risk-based budget and schedule, and use a benefit-cost approach to selecting the best available alternative within the budget.

The benefit-cost analysis is supposed to be a formal, systematic, economic assessment of each alternative solution based on the net present value of all quantifiable benefits and costs. The solutions should be ranked based on the discounted net present value of the benefits less the costs, and include some attempt to quantify the risk associated with the assumptions used to estimate benefits and costs.

This is clearly a complicated and time consuming process, and is not something that could have been completed in a matter of weeks. At the time we issued our Flash Audit Alert in June 2015, many of the activities had not been completed in support of a properly developed Business Case. We expressed the opinion that OPM's desire to better secure its IT environment as quickly as possible, and therefore declining to perform many of the mandatory planning steps, resulted in a high risk that the Project would fail to meet its objectives. Now that we have reviewed OPM's recent Business Case and its supporting

activities in depth, we are even more concerned about the lack of disciplined capital planning processes.

OPM did not initially convene an integrated project team (although one has since been appointed) or complete the proper market research and analysis of alternatives before deciding to abandon OPM's legacy environment and embark on its IaaS effort. We were told by OCIO staff that OPM's former Chief Information Officer discussed possible alternatives with her staff, with input from Imperatis (the contractor that was hired to help secure OPM's legacy environment in the wake of the April 2014 data breach) in selecting this alternative. However, no documentation was provided to us to support this assertion.

Furthermore, OPM did not develop a realistic budget based on an understanding of the number of systems that would need to be migrated to the new environment, the level of effort associated with the required modernization and security updates, and the cost of this process (See Section B. for further discussion). Another critical requirement of the capital planning process is not only to develop realistic life-cycle cost estimates for the capital asset, but also to assess the political support for those costs. It would not make sense to initiate a major project potentially costing hundreds of millions of dollars without first understanding whether OMB would support, and the Congress would appropriate, funding for the project.

As reported in our first interim status report in September 2015, OPM informed us in April 2015 that it had extensive discussions with OMB about this project, and that its project plan had been approved by OMB and other agencies involved in cybersecurity. When we asked for a copy of the project plan that had been provided, we were given what was essentially a list of security tools that OPM planned to purchase, not something that could be considered any type of planning document, project charter, or business case for the Project. We also asked OPM to provide evidence to document the nature of its meetings with OMB. OPM has not provided any documentation, even though it claims that "extensive discussions" took place with OMB.

In any event, it is clear that OPM initiated this major IT project without following the proper procedures. In the wake of the April 2014 data breaches, OPM decided on a course of action without following the required capital planning procedures. We recognized that there was a sense of urgency after discovering that a breach had occurred and agreed that it was critical to secure the legacy environment as quickly as possible (this was the first, or Tactical, phase of the Project). However, once the legacy environment was stabilized, OPM should have conducted the appropriate Project planning steps required by OMB Circular A-11, especially developing the Project budget and analysis of alternatives.

A further complication is the recent decision by the PAC-PMO, after its 90-day review,[2] to create the National Background Investigations Bureau, an independent component of OPM, and transfer responsibility for the IT systems that support the background investigations business process to the Department of Defense. Our understanding is that OPM planned to use its revolving fund, which derives the majority of its revenues from background investigations, to fund a significant portion of the costs of the Project. However, since the IT systems that support background investigations processing will now not be part of the IaaS, it would seem that a large portion of the planned funding source will not be available for the Project.

As a result of OPM's failure to perform proper capital planning activities, especially developing a realistic estimate of the Project's life cycle costs and conducting the appropriate analysis of alternatives, we continue to believe that there is a very high risk that the Project will fail to meet its stated objectives of delivering a more secure environment at a lower cost.

It is still not too late, however, for OPM to complete the activities that should have been done before it initiated this Project. This is even more important given the changes that have occurred. OMB guidance for completing a Business Case states that "significant changes . . . should be reflected in an updated investment-level Alternatives Analysis, subject to OMB review."

Recommendation 1

We recommend that OPM complete an Analysis of Alternatives as described in the Capital Programming Guide supplement to OMB Circular A-11 as soon as possible. This analysis should recognize changes in the internal and external environment and no consideration should be given to funds already spent associated with the Project (i.e., avoid the sunk cost fallacy).

OCIO Response:

In its response to the draft report, the OCIO stated that:

"OCIO agrees that conducting such an AOA going forward, including looking at alternatives to "Shell" for mitigating, migrating, or modernizing legacy applications and infrastructure, would be beneficial to OPM and bring enhanced rigor to the capital planning process. It is particularly beneficial in light of the recent decision to transition

[2] The Suitability and Security Performance Accountability Council Program Management Office (PAC-PMO) is an interagency group chaired by OMB and comprised of the Director of National Intelligence and the OPM Director in their respective roles as Security and Suitability Executive Agents. In the wake of the OPM data breaches, the PAC-PMO initiated a 90-day review of the suitability and security clearance process.

background investigation services to the National Background Investigations Bureau (NBIB) and have DOD provide the IT support to the NBIB."

The OCIO's response also outlined the additional steps it plans to take to improve its capital planning process, including:

- ***Creating and updating application profiles and conducting reviews of major IT systems, prioritizing High-Value Assets (HVAs). As part of these reviews, OPM plans to complete and document an Analysis of Alternatives in which migration to "Shell" will be considered against other alternatives.***
- ***Applying a similar Analysis of Alternatives with respect to data center consolidation. Looking at each data center, OCIO plans to consider migration to Shell against other alternatives, such as mitigation or modernization of the legacy infrastructure, and/or migration to alternative environments.***
- ***Instituting an updated process to ensure that IT business cases are aligned with OMB A-11 and other modern IT practices for other existing and future projects.***
- ***Adopting an Agile methodology in which iterative development cycles would provide feedback to form the basis of subsequent activity.***

OIG Reply:

We acknowledge that OPM officials agree with our recommendation, and commend them for their thoughtful response and detailed plan to implement it. The Agile development methodology is envisioned, and in fact encouraged, in OMB's budget guidance in which the concept of 'useful project segments' is applied to capital financing principles. We emphasize, however, that an Agile approach should be balanced with the need for structured development and budgeting principles. We will continue to closely monitor OCIO's efforts to improve its capital planning process as it relates to the Project.

B. Lifecycle Cost Estimates

As briefly discussed in the previous section, a critical component of the capital asset planning process is estimating the full lifecycle costs of a major IT initiative. This is true for two reasons. First, estimating the full lifecycle costs allows the development of a baseline for evaluating feasible alternative solutions. Second, it provides sufficient information so the agency may seek a funding commitment for the lifecycle of the project (or at least for major useful segments) before committing to its implementation.

A prerequisite to estimating the lifecycle costs of the Project requires that OPM first fully understand its scope, which means that OPM would have to conduct a complete inventory of systems, and have an understanding of their technical architecture and the level of effort

required to migrate or modernize them. Only after this critical, but understandably complex, process is completed can a realistic cost estimation be done. OPM, however, initiated the Project before completing this process.

OPM's Business Case submitted to OMB with the FY 2017 budget request outlines the costs already incurred for this Project along with reasonable short-term cost estimates to finish developing the IaaS portion. However, its cost estimates for modernizing and migrating its information systems to the new environment are unsubstantiated because of the incomplete inventory and technical analysis. OPM officials have candidly informed us that their cost estimates are "best guesses." In our opinion, these cost estimates significantly understate the true costs of the Project.

Another problem is the limited amount of funding that OPM is allocating to its modernization and migration effort. The IaaS Business Case contains budget projections that allocate the majority of funds toward three primary areas: maintaining the legacy environment, maintaining the new IaaS environment, and modernizing and migrating OPM's information systems. For FYs 2017 through 2020, the budget allocates approximately 20 to 25 percent of the Project's IT costs to modernization/migration, while the rest is dedicated to concurrently securing and maintaining the legacy and IaaS environments.

However, this approach does not seem to consider the fact that maintenance costs for the dual environments will not likely remain fixed. As these two environments continue to age, the costs of keeping them functional and secure will continue to increase. Eventually, maintenance costs could consume OPM's entire budget for the Project, leaving no funding available for modernization and migration. We addressed this potential worst-case scenario in our June 2015 Flash Audit Alert by warning that the agency's approach could force it to indefinitely support both the IaaS and its legacy environment. This would further stretch already inadequate resources, and therefore make both environments less secure and susceptible to another data breach.

Because OPM's lifecycle cost estimates are unsupported and probably significantly understated, there is a high risk that future budgets will continue to be inadequate to complete the Project. This increases the likelihood of the "worst case scenario" mentioned above, unless OPM decides to simply move its legacy systems into the IaaS without first modernizing and updating their security and operational features. While this may mitigate the cost impact of maintaining dual environments, it would not be consistent with the original Project goals.

We recently became aware of a plan to physically move legacy systems from the old data centers into the new data centers, but keep them in a separate logical environment from IaaS.

While on the surface this seems like a reasonable plan to save money in the short term, it does not significantly reduce the risks associated with maintaining security controls in two logical environments indefinitely.

Another impact of OPM's inadequate project planning is the potentially wasteful spending that has occurred in creating an IaaS environment before it was clear that it was the best solution, and before the technical analysis of the scope of the effort was completed. OPM is currently spending approximately $25 million annually to maintain the IaaS.

While OPM has not yet determined the full scope of this Project, there has been some improvement in developing an inventory of legacy systems and estimating the costs to modernize them. OPM's Senior Cybersecurity and Information Technology Advisor to the Director has developed a framework that we are optimistic can begin to provide OPM with this critical information. This "application profiling" scoring approach not only provides a means to evaluate the urgency of modernizing or migrating individual information systems, but also includes the critical step of estimating the costs associated with each application.

While this type of analysis should have occurred before heavily investing in IaaS, we are pleased to see that OPM at least has a framework in place to begin developing true cost estimates for this Project. With this information in hand, OPM will be in a position to develop a realistic lifecycle cost estimate as input to the analysis of alternatives discussed in Section A and Recommendation 1.

Recommendation 2

We recommend that OPM leverage the application profiling scoring framework to develop cost estimates for modernizing and/or migrating all OPM information systems, and use this information to support the capital planning activities referenced in Recommendation 1. The Business Case should be continuously updated to reflect these cost estimates as they become more concrete.

OCIO Response:

"OPM also concurs with the OIG's recommendation that the agency would benefit from more rigorous estimation of lifecycle costs. To achieve this, OPM IT Program Managers plan to use the application profile framework designed by OPM's Senior Cybersecurity and Information Technology Advisor to inform lifecycle cost estimation for modernization projects. As we continue to develop our cost estimates, we will continue to seek feedback from partners such as the Office of Management and Budget and the OIG."

OIG Reply:

We agree with the approach of using the high-value asset application profile framework to estimate modernization costs on a system by system basis, but these efforts should be based upon recognized cost estimation principles and procedures.

If you have any questions about this interim status report, please contact me, at 606-1200, or someone from your staff may wish to contact Michael R. Esser, Assistant Inspector General for Audits, at [redacted].

Appendix

cc: Kiran A. Ahuja
Chief of Staff

Kathleen M. McGettigan
Chief Management Officer

Lisa Schlosser
Acting Chief Information Officer

Clifton N. Triplett
Senior Cybersecurity and Information Technology Advisor

Janet L. Barnes
Director, Internal Oversight and Compliance

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

APR 2 2 2016

MEMORANDUM FOR MICHAEL R. ESSER
Assistant Inspector General for Audits

FROM: LISA SCHLOSSER
Acting Chief Information Officer

SUBJECT: CIO Response to the Second Interim Status Report on the U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project

Introduction

The OPM Office of the Chief Information Officer (OCIO) has reviewed the Second Interim Status Report on the U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project. The OCIO appreciates the detailed analysis and feedback provided in the report, and generally concurs with the recommendations. This response focuses on the efforts underway, and planned next steps, to address the recommendations.

Since the Office of the Inspector General (OIG) issued the first Flash Audit Alert on the status of OPM's Infrastructure Improvement Project last summer, we have already begun to address OIG concerns. As the OIG has noted, OPM has:

- Submitted an updated OMB Major Information Technology Business Case for the Infrastructure Improvement Project;
- Engaged in on-going efforts to inventory IT systems and identify plans to mitigate, migrate, or modernize these systems; and
- Drafted an Application Profile methodology and process that assesses potential IT system risk while migrating and modernizing OPM IT applications. As discussed in more detail below, this will inform the development of a more comprehensive lifecycle cost estimate for IT applications and for the Infrastructure Improvement Project.

As the OIG acknowledges, OPM embarked on the Infrastructure Improvement Project with a "sense of urgency" following the 2014 data breach. OPM previously concluded that it was critically important to take the appropriate steps to better secure OPM's aging legacy infrastructure in the near term, while putting in place a longer-term solution to transition its infrastructure into a more secure, modern environment. OPM consulted with its interagency partners, including the Department of Homeland Security and the Office of Management and Budget, as it developed its new "Shell" or IaaS environment.

As the OIG points out, however, OPM did not conduct a formal Analysis of Alternatives (AOA) at the time. OCIO agrees that conducting such an AOA going forward, including looking at alternatives to "Shell" for mitigating, migrating, or modernizing legacy applications and infrastructure, would be beneficial to OPM and bring enhanced rigor to the capital planning process. It is particularly beneficial in light of the recent decision to transition background investigation services to the National Background Investigations Bureau (NBIB) and have DOD provide the IT support to the NBIB. As previously discussed with the OIG, it has been, and continues to be, OPM's intent to utilize an agile methodology that is iterative in nature and that allows us to continue to adapt to evolving needs, circumstances, and technologies. Consequently, in accordance with the OIG's recommendations, OPM OCIO intends to take the following actions:

Recommendation 1: Capital Planning Process Improvement Plan

OPM concurs with Recommendation 1 and has initiated and plans to continue to implement the following steps to enhance our Capital Planning Process:

1) OPM OCIO is creating and updating application profiles and conducting reviews of major IT systems, prioritizing High-Value Assets (HVAs). These reviews are designed to assess risk and to meet the standards of OMB Circular A-11 and other modern IT practices. As part of these reviews, OPM plans to complete and document an AOA in which migration to "Shell" will be considered against other alternatives. These alternatives may include mitigation or modernization of the legacy system, and/or migration to other environments that are or may become available in the future, such as a commercial or government cloud.
2) As part of its ongoing efforts to rationalize its infrastructure and reduce costs, OPM OCIO plans to apply a similar AOA with respect to data center consolidation. Looking at each data center, OCIO plans to consider migration to Shell against other alternatives, such as mitigation or modernization of the legacy infrastructure, and/or migration to alternative environments. After OCIO completes its review of its legacy data centers, it plans to then conduct an AOA for the new "Shell" data centers in [redacted] and [redacted], to determine whether these data centers should continue to be utilized, be scaled differently, or migrated to a different environment.
3) For existing and future projects, the OPM OCIO, in coordination with the OPM Investment Review Board, plans to institute an updated process to ensure that IT business cases are aligned with OMB A-11 and other modern IT practices.

We are taking an agile approach to these plans, working in iterative cycles in which feedback on our progress in one stage will inform our approach to the next. For example, we anticipate that the first stage of our infrastructure review will evaluate alternative paths to modernization for one of the data centers in our legacy infrastructure environment. We will share the results of this first stage of analysis with the OIG for feedback on our approach.

Collectively, these steps will have two benefits for OPM. First, they will help ensure that the future architecture and management of the Infrastructure Improvement Project is rigorous, and that OPM makes the most cost-effective decisions for transitioning out of the legacy environment while maintaining a strong security posture. Second, these actions lay the groundwork for better investment management processes in the future.

Recommendation 2: Lifecycle Cost Estimate Improvement Plan

As stated above, OPM also concurs with the OIG's recommendation that the agency would benefit from more rigorous estimation of lifecycle costs. To achieve this, OPM IT Program Managers plan to use the application profile framework designed by OPM's Senior Cybersecurity and Information Technology Advisor to inform lifecycle cost estimation for modernization projects. As we continue to develop our cost estimates, we will continue to seek feedback from partners such as the Office of Management and Budget and the OIG.

These profiles, which are currently in their first iteration, will allow OPM to prioritize systems for modernization by using the NIST FIPS 199 and the OMB HVA evaluation criteria to rate them as low, medium, or high priority across a number of dimensions. Some of these dimensions, such as process complexity and technical obsolescence, are "drivers" of modernization. Other dimensions, such as feasibility and funding source, are "challenges" to modernization. OPM will consider these profiles when making modernization funding decisions and will update business cases for Major IT Investments as necessary.

Conclusion

As we continue to implement these and other improvements, the OPM OCIO will share the results with the OIG on a frequent basis, to include providing on-going updates as part of the bi-weekly meeting agenda.

If you have questions about this report, I encourage you to contact me directly at [redacted]. We look forward to further discussions on this topic.

cc: Kiran A. Ahuja
Chief of Staff

Kathleen M. McGettigan
Chief Management Officer