UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

May 27, 2009

Report No. 4A-CI-00-09-053

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND Patrick E McFarland
Inspector General

SUBJECT: Flash Audit Alert – Information Technology Security Program at the U.S. Office of Personnel Management

Synopsis

The Office of the Inspector General (OIG) at the U.S. Office of Personnel Management (OPM) is issuing this flash audit alert to bring to your immediate attention serious concerns that we have with OPM's information technology (IT) security program. Specifically:

- OPM's Center for Information Services (CIS) misrepresented the status of the agency's IT security program in the FY 2009 second quarter Federal Information Security Management Act (FISMA) report issued to the U.S. Office of Management and Budget (OMB).
- OPM's IT security policies and procedures continue to remain severely outdated.
- OPM's IT security program is understaffed, and the agency has operated without a permanent IT security officer (ITSO) for over 14 months. In addition several individuals within the IT security program do not have adequate independence from other OPM program offices.

The impact of these concerns is two-fold. First, misrepresenting the status of any component of OPM's IT security structure could result in the loss of integrity and confidence in OPM's overall IT security program. Secondly, without current IT security policies and procedures, as well as a dedicated and experienced ITSO and support staff, OPM's IT security program will become ineffective, thereby compromising the confidentiality, integrity, and/or availability of information being processed, stored, or transmitted by OPM's major applications and systems. We believe that this misrepresentation of the security status exemplifies the risk of operating an IT security program with outdated controls and without a permanent ITSO for an extended period of time.

We discussed these issues with OPM's Chief Information Officer (CIO) and senior managers in the CIS program office, and considered their comments in the preparation of this report. In order to verify that the audit concerns are addressed in a timely manner, we ask that CIS respond directly to the OIG within 60 days of the date of this report advising us of any progress made in implementing the audit recommendations.

If we can be of assistance during the program office review of this report, the staff should contact Michael Esser, Assistant Inspector General for Audits, on [redacted]. Please call if I can be of further assistance to you.

Executive Summary

Our review of OPM's quarterly FISMA report for the second quarter of 2009 resulted in serious concerns. This led to an in-depth audit of the FISMA reporting process and other areas related to OPM's IT security program. As a result of this audit, we noted several critical issues related to the FISMA quarterly reporting process, IT security policy, and the overall management of OPM's IT security program.

OMB requires agencies to submit quarterly status reports on their plan of action and milestones (POA&M) process, IT security performance measures, privacy, and the criteria for "maintaining green" on the eGOV portion of the President's Management Agenda scorecard. OPM's FY 2009 second quarter report was submitted to OMB on March 1, 2009. Our audit of this report showed that it significantly misrepresented OPM's IT security status regarding the POA&M process. In addition, OPM's IT security program continues to operate with outdated policies and procedures and without a permanent ITSO.

This flash audit alert details the issues that were detected and recommendations for improvement. In summary:

- Two major applications owned by the Human Resources Line of Business (HRLOB) program office were migrated to a new hosting provider in July 2008, which required out-of-cycle certification and accreditation (C&A) of both systems. These systems are the Electronic Official Personnel Folder (eOPF) and the Enterprise Human Resources Integration (EHRI) Data Warehouse.
    - HRLOB believed that some of the overdue POA&M items for both systems should be closed because they were no longer relevant post-migration, and were working with CIS representatives to this end.
    - The program office submitted its FY 2009 second quarter POA&M reports for both systems to CIS on January 27, 2009. The reports continued to itemize all existing weaknesses, including 48 that were more than 120 days overdue. CIS contractors, however, unilaterally and without discussing the approach with the program office, closed all POA&M items and used the POA&M reports that were created during the certification and accreditation process for both systems as supporting documentation for the FY 2009 second quarter FISMA report to OMB.
- On the FY 2009 second quarter FISMA report to OMB, CIS inappropriately reported the number of POA&M ***weaknesses*** with overdue corrective action rather than the number of ***systems*** where corrective action has been delayed (as required by OMB).

- OPM's IT security policies and procedures continue to remain severely outdated, as many have not been updated at all in at least three to six years. The OIG has reported this issue to the OPM Director for the past three years, and labeled it as a material weakness in the FY 2007 and FY 2008 FISMA reports to OMB.
- OPM has operated without a permanent ITSO for over 14 months, and there have been 3 acting ITSO's during that time. In addition, the responsibilities assigned to the current acting ITSO create the appearance of a lack of independence in that he is responsible for managing OPM's network infrastructure and also responsible for oversight of its IT security compliance.

Audit Results

I. FY 2009 Second Quarter FISMA Report – POA&M Process

The POA&M section of the quarterly report instructs agencies to list the number of systems where planned corrective action on security weaknesses is overdue. In OPM's FY 2009 second quarter report, we found two problems in the manner overdue items were reported. First, the CIS did not report overdue corrective action for two OPM systems: eOPF and the EHRI Data Warehouse. Second, CIS reported the number of weaknesses with overdue corrective action rather than the number of systems where corrective action has been delayed.

a) eOPF and EHRI Data Warehouse POA&M Weaknesses

We noted significant discrepancies between the FY 2009 second quarter report to OMB and the POA&M reports that the HRLOB program office submitted to CIS for the eOPF and EHRI Data Warehouse systems. The OMB report showed no overdue weaknesses for the two systems, while the POA&M reports submitted by the HRLOB program manager on January 27, 2009 showed that there were 19 items where corrective action was more than 120 days overdue for the eOPF system, and the EHRI Data Warehouse POA&M identified 29 security weaknesses with overdue corrective actions.

We interviewed program office officials and CIS representatives, and reviewed associated documentation to determine the cause of this discrepancy. Our review demonstrated that the facts of the situation are as follows:

Both eOPF and the EHRI Data Warehouse systems were migrated to a Denver, Colorado area hosting facility owned by the Department of the Interior. As a result of this change, an out-of-cycle C&A for both systems was triggered. These C&A's were completed during the summer and fall of 2008, and the official authority to operate for both systems was executed in November 2008 for the EHRI Data Warehouse and January 2009 for eOPF.

Sometime after the system migration in June 2008, the HRLOB program office began discussions with CIS to close out certain POA&M items that it believed were no longer relevant. The program office requested that 24 of the 29 overdue items be closed on the EHRI Data Warehouse POA&M. These discussions continued, but there was no definitive resolution of the status of these POA&M items, and they therefore remained as open and overdue weaknesses on the system's POA&M report.

During this same timeframe, there were changes occurring in the CIS group responsible for managing the agency-wide POA&M process. Working under the Chief of CIS's Program Policy Group, a Federal employee and one or more contractors obtained quarterly POA&M reports for the 40 OPM major computer systems, reviewed corrective action and proof-of-closure documentation, and monitored quarterly metrics on a "POA&M Status Tracker" matrix. This team was responsible for recommending whether POA&M items should be closed or, if insufficient documentation was received, kept open.

About five days before the FY 2009 second quarter report was due to be submitted to OMB, CIS management reassigned this process to several Network Management Group (NMG) network security contractors under the direction of a new acting ITSO. We were told that this change was put in place because of management concern over the high number of unresolved POA&M weaknesses; however, nothing came to our attention that would allow us to definitively conclude that this was the reason.

The NMG contractors were directed to focus their efforts on reviewing the POA&M items where corrective action was more than 120 days overdue. Since a significant portion of these items was attributable to eOPF and the EHRI Data Warehouse, the contractors seemed to target these two systems for further review.

There is one additional complication related to the eOPF POA&M. This system is a web-based application that allows Federal employees and agency human resources professionals to view digital copies of official personnel documents. Although the infrastructure supporting the application is now hosted by the Department of Interior's National Business Center, there are two sub-systems involved in the process of digitizing the documents that were not directly affected by the system migration. The eOPF POA&M submitted by the HRLOB program office includes weaknesses related to the application as well as both sub-systems.

However, the C&A process that occurred in the summer and fall of 2008 only covered the eOPF application itself and not the two sub-systems. One of the deliverables resulting from this C&A, and the EHRI Data Warehouse C&A, was a document prepared in the standard POA&M format that included security weaknesses identified during the C&A process. This document did not include previously identified security weaknesses for eOPF (or its two sub-systems) or the EHRI Data Warehouse.

Nevertheless, the NMG contractors who were assigned to manage the POA&M process used these documents as a basis for preparing OPM's FY 2009 second quarter FISMA report rather than the POA&M reports that had been submitted by the HRLOB program office. A memo dated February 15, 2009 from one of the contractors to CIO Janet Barnes described the reasoning for relying on the C&A version of the POA&Ms, but it only addressed the eOPF application POA&M, and did not account for the items related to the subsystems that were overlooked. We also interviewed the contractor to determine why the program office POA&Ms were not used as source documentation for the FY 2009 second quarter FISMA report.

Based on the memo and on our interview, we understand that the NMG contractors believe that when a system undergoes a major change that requires an out-of-cycle certification and accreditation, a new POA&M is in order. The thought process is that a major change, especially one involving a new hosting provider, can involve new management, infrastructure, and staff, rendering the existing POA&M weaknesses irrelevant.

While this may be true in some cases, it is not a universally valid concept. For example, there were 29 items on the EHRI Data Warehouse POA&M submitted by HRLOB that were over 120 days overdue. Of these, only 17 items related to the system migration. Even if CIS were justified in closing these items, they should have remained on the POA&M in a "closed" status for one year for tracking purposes. The remaining 12 overdue items do not appear to have a direct relationship with the system migration, but they were closed and reopened with future completion dates.

In addition to the overdue weaknesses related to the eOPF subsystems that were overlooked, there were four POA&M items reported on the HRLOB POA&M submission that CIS inappropriately closed. These items related to security impact analysis, multifactor authentication, public key certification, and system output. These are items that would not be directly alleviated or become irrelevant as a result of a physical system migration, and should continue to be listed as weaknesses on post-migration POA&Ms.

These examples clearly demonstrate that some of the overdue POA&M items for these two systems should not have been closed. In fact, this was the nature of the discussions that occurred between CIS and HRLOB during the fall of 2008. The CIS representatives who previously managed the POA&M process were working with program office officials to determine which POA&M items should be appropriately closed after the system migration of summer 2008. This process involved a careful review of each POA&M item and "proof of closure" submitted by the program office to support closing the items.

However, the NMG contractors inappropriately closed all overdue POA&M items on both systems without discussing their status with the HRLOB program office. The memo to the CIO was written to justify this course of action, but no proof of closure was provided (although the memo referenced supporting documentation that was on file). When we interviewed HRLOB program office officials, they stated that they had no knowledge of the modified POA&Ms for the eOPF and EHRI Data Warehouse systems, and had no discussions with CIS after the reorganization occurred in late February 2009.

Surprisingly though, CIS and HRLOB resumed discussions regarding the closure of POA&M items that were rendered obsolete by the summer 2008 system migration after the POA&Ms had been modified by CIS and the FY 2009 second quarter FISMA report was submitted to OMB. When we asked CIS officials why there were discussions on this topic after the NMG contractors had already determined that all POA&M items were no longer relevant and should be closed, there was no reasonable response provided.

OMB Memorandum M-04-25, Section B.I "Agency Plans of Action and Milestones Process" provides a sample POA&M and instructions on completing the various columns. The memo states "Once an agency has completed the initial POA&M, no changes should be made to the data in columns 1, 4, 5, and 7."

The memo continues with specific descriptions for each column:

- "Column 4 – Scheduled completion date for resolving the weakness. Please note that the initial date entered should not be changed. If a weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in Column 8, 'Status.'
- "Column 5 – Key milestones with completion dates. A milestone will identify specific requirements to correct an identified weakness. Please note that the initial milestones and completion dates should not be altered. . . .
- "Column 8 – Status. The agency should use one of the following terms to report status of corrective actions: Ongoing or completed. 'Completed' should be used only when a weakness has been fully resolved and the corrective action has been tested. Include the date of completion. . . ."

In the Frequently Asked Questions section of M-04-25, it states, "For how long do I report corrected weaknesses?

"Weaknesses that are no longer undergoing correction and have been completely mitigated for over a year should no longer be reported in the agency POA&M."

OMB Memorandum M-08-021 "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" also includes a Frequently Asked Questions section.

Question 34 states, "Can a POA&M process be effective even when correcting identified weaknesses is untimely?

"Yes. The purpose of a POA&M is to identify and track security weaknesses in one location. A POA&M permits agency officials and oversight authorities to identify when documented corrective actions are both timely and untimely. In either circumstance, the POA&M has served its intended purpose. Agency managers can use the POA&M process to focus resources to resolve delays."

It is the clear intention of OMB that POA&M items are not to be modified, unless they are fully completed and tested. When items are resolved, it has been OPM's practice to mark them as "Completed" in the status column, shade the row with a green background, and maintain these items on POA&M reports for one year after the completion date. CIS has been very outspoken regarding these requirements during monthly meetings of the Information Technology Security Working Group (ITSWG).

Unresolved items that are overdue are shaded with a red background and bi-weekly status reports to the OPM Deputy Director are required until corrective action has been completed and tested. As stated in the OMB memorandum, the purpose of highlighting weaknesses where corrective action is significantly overdue is to focus management attention and necessary resources to resolve the items.

The CIS approach to the eOPF and EHRI Data Warehouse POA&Ms appears to have violated the intention of both the OMB POA&M guidance and OPM's own internal practices.

b) Reporting Total Number of Weaknesses instead of the Number of Systems with Weaknesses

The instructions within the FISMA quarterly reporting template ask for the: "Number of High, Moderate and Not Categorized systems operating with one or more security weaknesses that are currently 90 to 120, or greater than 120 calendar days beyond the planned remediation date in the POA&M." This section contains two columns; one in which to enter the number of systems that have POAM weaknesses 90-120 days overdue, and one in which to enter the number of systems with POAM weaknesses over 120 days overdue.

On the FY 2009 second quarter FISMA report to OMB, CIS reported the number of ***weaknesses*** with overdue corrective action rather than the number of ***systems*** where corrective action has been delayed. There are two factors that led to the OIG's conclusion that CIS incorrectly completed this section of the FISMA reporting template:

- CIS maintains an internal tracking spreadsheet that contains a detailed analysis of the POA&M status for each of the systems in OPM's inventory. This spreadsheet outlines the total number of delayed weaknesses for each system. The "totals" row for each program office lists the number of total overdue weaknesses for all systems owned by that program office. The numbers documented on the FY 2009 second quarter FISMA report match the total number of weaknesses outlined in this summary spreadsheet instead of the total number of systems containing any overdue weaknesses.
- In some cases, the number reported on the FY 2009 second quarter FISMA report in the field "Number of...systems...operating with one or more security weaknesses..." was greater than the number of systems that exist in that program office. For example, it was reported that the Federal Investigative Services Division (FISD) had 5 systems with weaknesses 90-120 days overdue and 6 systems with weaknesses over 120 days overdue, for a total of 11 systems. However, FISD only owns a total of 5 systems.

c) Summary

The POA&M section of the FY 2009 second quarter FISMA report understated weaknesses with corrective action overdue by more than 120 days. Additionally, CIS mistakenly reported the number of overdue weaknesses rather than the number of systems with overdue weaknesses.

We believe that the factors that led to these conditions are, at least in part, related to outdated and incomplete IT security policies and long-standing weaknesses in OPM's IT security management structure. Both of these issues have been the subject of OIG audit findings since FY 2006 (please see sections II and III of this Flash Audit Alert).

As a result, the OPM Director and OMB were given an inaccurate representation of OPM's IT security position. The decision memorandum transmitting the FY 2009 second quarter FISMA report to the OPM Director claimed a 53 percent improvement in POA&M corrective actions delayed past their scheduled completion date, and a 46 percent decrease in the number of 120-day old corrective actions from the first quarter. While it may be true that some of the overdue POA&M items for eOPF and the EHRI Data Warehouse would have eventually been closed following the migration to the new hosting facility, this process was not properly completed before the memorandum was sent. Also, if the POA&M items related to the two eOPF subsystems had been included, the number of overdue weaknesses would have actually increased in the second quarter. Therefore, the improvements claimed in the decision memorandum are not entirely accurate.

Recommendation 1

We recommend that CIS correct the FY 2009 second quarter FISMA report to accurately reflect the status of OPM's IT security position as of March 1, 2009. This would include reporting that eOPF and the EHRI Data Warehouse systems both have weaknesses more than 120 days overdue, and changing the metrics on the entire report from the number of overdue weaknesses to the number of systems with overdue weaknesses.

II. OPM IT Security Policy

The CIS closely follows emerging IT security guidance, and disseminates this information to the agency's IT security personnel through monthly meetings of the ITSWG. However, OPM's IT security policies and procedures remain severely outdated. In fact, the majority of these documents have not been updated at all in at least three years.

According to the decision memorandum that accompanied the FY 2009 second quarter FISMA report, CIS has developed guidance and training materials related to the POA&M process and is working on a set of comprehensive POA&M standard operating procedures. Although these would be welcome developments, the same effort needs to be directed toward developing a comprehensive set of OPM IT security policies and procedures that are updated at least annually.

National Institute of Standards and Technology Special Publication (NIST SP) 800-100, Information Security Handbook: A Guide for Managers, states that "An effective information security governance program requires constant review. Agencies should monitor the status of their programs to ensure that . . . Policies and procedures are current and aligned with evolving technologies, if appropriate . . . Over time, policies and procedures may become inadequate because of changes in agency mission and operational requirements, threats, environment, deterioration in the degree of compliance, changes in technology or infrastructure, or business processes."

We acknowledge the steps that OPM has taken in working toward updating policies, and we understand the impact that limited resources can have on the ability to conduct this type of ongoing maintenance. However, OPM's failure to adequately update IT security policies and procedures has been highlighted in the past three OIG FISMA audit reports, and was characterized as a material weakness in the FY 2007 and FY 2008 FISMA reports.

CIS must address this underlying weakness in information security governance, or there will likely be repeated occurrences of the problems that occurred with the FY 2009 second quarter FISMA report. In this situation, there was new staff attempting to understand the POA&M and C&A processes, but there was the no formal guidance that they could use as a reference.

Recommendation 2

We recommend that CIS develop a comprehensive set of IT security policies and procedures, and a plan for updating it at least annually.

III. OPM IT Security Management

While we believe that CIS is committed to developing and maintaining strong IT security controls, it is clear that there are opportunities for improvement in the overall leadership and management of the IT security program. The agency has operated without a permanent ITSO for over 14 months, and there have been 3 acting ITSO's during that time.

This is a position that requires an independent, long-term, and committed incumbent to manage the complexities of an environment that includes constantly shifting guidance and a group of program office representatives with a wide range of IT security experience. Adequate support staff is also needed to effectively manage the agency's IT security program.

In contrast, the new acting ITSO and recently-assigned staff are not independent. The acting ITSO is also the Director of the Network Management Group, a program office that manages one of the two major IT infrastructure elements at OPM. The staff includes two NMG network security contractors. There are also two federal employees.

This situation creates the appearance of a lack of independence in that officials who are responsible for one of the largest and highest-risk major systems are now also responsible for oversight of the IT security compliance of that system. We have learned that the acting ITSO will not be responsible for accreditation decisions related to any systems under his purview, and that the CIO will take on that role in these cases. This appears to be an attempt to mitigate conflict of interest concerns that have already been raised; however, we do not believe this to be a workable solution. In our view, the CIO has far too many responsibilities to be involved at the level of detail required to make informed decisions in these matters.

We have recently learned that the former OPM Acting Director approved a reorganization in CIS that creates an IT Security and Privacy Group reporting to the agency's CIO. This is a positive development; however, the ITSO position is still vacant and it is not clear how the group will be staffed.

NIST SP 800-37 states, "The *senior agency information security officer* is the agency official responsible for: (i) carrying out the Chief Information Officer responsibilities under FISMA; (ii) possessing professional qualifications, including training and experience, required to administer the information security program functions; (iii) **having information security duties as that official's primary duty** [emphasis added]; and (iv) heading an office with the mission and resources to assist in ensuring agency compliance with FISMA."

There are a number of underlying causes that have contributed to preventing OPM from adequately staffing an IT security program, including a lack of resources, budgeting issues, and especially difficulties related to the federal hiring process. However, CIS management must resolve these issues and correct this long-standing weakness.

Without strong information security governance, OPM cannot implement appropriate and cost-effective information security controls (beginning with current and comprehensive policies and procedures) or manage evolving information security risks. The problems that occurred with the FY 2009 second quarter FISMA report are an example of what can occur without strong information security governance.

Recommendation 3

We recommend that the OPM Director ensure that CIS has adequate resources to properly staff its IT Security and Privacy Group.

Recommendation 4

We recommend that CIS recruit a permanent Senior Agency Information Security Officer as soon as possible, and adequate staff to effectively manage the agency's IT security program.

cc: Elizabeth A. Montoya
Chief of Staff and Director of External Affairs

Richard B. Lowe
Deputy Chief
of Staff and Executive Secretariat

Ronald C. Flom
Associate Director, Management Services Division and
Chief Human Capital Officer

Janet L. Barnes
Deputy Associate Director
Center for Information Services and Chief Information Officer

David M. Cushing
Deputy Chief Financial Officer