UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

September 28, 2009

Report Number: 4A-CI-00-09-066

MEMORANDUM FOR JOHN BERRY
Director

FROM PATRICK E. McFARLAND
Inspector General

SUBJECT: Review of the Consolidated Business Information System Implementation Project

Background

The purpose of this memorandum is to communicate to you the findings and conclusions resulting from our review of the Consolidated Business Information System (CBIS) project. You asked us recently to review this project to identify any serious issues that could potentially jeopardize the successful implementation of the new system. Our review was limited to Phase 1 Release 1 of the project, scheduled for implementation in October 2009 and focusing on the U.S. Office of Personnel Management (OPM) Revolving Fund and Salaries and Expenses accounts.

Our approach was to identify and review critical tasks associated with the project. We determined these to include project management, testing, independent verification and validation (IV&V), data conversion, information technology (IT) certification and accreditation, operational readiness, compliance with Federal Systems Integration Office (FSIO) requirements and OPM custom requirements, and application security.

The responsibility for reviewing these critical tasks was separated between the Office of the Inspector General (OIG); SRA International, Inc. (SRA), the IV&V contractor; and KPMG. The OIG's area of responsibility was to review five sub-tasks within the overall critical tasks identified above. These included staff training, project risk management, resolution of IV&V issues, IT certification and accreditation, and the overall testing strategy. SRA's ongoing responsibilities included verification that all necessary testing is completed and validation of the data conversion reliability. SRA provides CBIS project managers routine reports summarizing their conclusions. KPMG was responsible for evaluating the overall project management strategy (including compliance with best practices and applying earned value management), tracing requirements to testing, role of the IV&V contractor, the data conversion strategy, operational readiness, compliance with FSIO requirements, and application security. KPMG is currently finalizing its review and will report their results independently. Preliminary results will be provided on October 2, 2009, followed by final results on October 16, 2009. At this point, KPMG has not reported any significant issues.

This review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however because we consider this to be a review, the documentation, reporting, and quality control standards are not as stringent.

Executive Summary

Overall, nothing came to our attention that caused us to believe that the CBIS project management office will not successfully implement CBIS Phase 1 Release 1 as scheduled in October 2009. However, we did note several opportunities for improvement in four of the five critical sub-task areas that the OIG reviewed:

- Project risk management: Although we believe that most project risks are properly managed, our examination of project risk meeting minutes and the risk inventory database revealed that several risks were closed without adequate documentation or justification.
- Resolution of IV&V issues: When there is disagreement concerning IV&V contractor recommendations, there is no resolution process. As a result, potential concerns may not be properly tracked and mitigated by the CBIS project management office within the Office of the Chief Financial Officer (OCFO).
- IT Certification and Accreditation (C&A): The CBIS C&A was conducted in accordance with OPM's Certification and Accreditation Guide and applicable guidance from the National Institute of Standards and Technology (NIST). However, we identified two areas where documentation could be improved:
  - As part of the C&A package, a privacy impact assessment (PIA) was conducted for CBIS in July 2009. U.S. Office of Management and Budget (OMB) Memorandum M-03-22 outlines the requirements of a PIA. Although the CBIS PIA contained the majority of the required elements, it did not include several requirements applicable to major information systems.
  - The CBIS contingency plan contains the majority of critical elements required by NIST guidance; however there are several discrepancies between two documents critical to the CBIS contingency planning methodology. In addition, we found that the contingency plans did not contain adequate contact information for personnel critical to the disaster recovery process.
- Overall testing strategy: We recommend that the CBIS project team improve the user acceptance testing process by:
  - providing better qualified Accenture personnel during the testing sessions; and
  - making the scripts user friendly by providing more descriptive information and screen shots of the functions that UAT participants are responsible for testing.

Results

1. Staff Training

The OCFO manages the CBIS user training program with assistance from Accenture, one of the contractors working on the project. The OCFO has developed a thorough training

methodology with adequate controls to ensure that all CBIS users receive the appropriate quality and quantity of training. Nothing came to our attention during this review to indicate that there are weaknesses in the CBIS training approach. The following sections detail our observations related to the CBIS training program.

a. Training Needs

The first objective of the CBIS training team was to document and understand the skill set needed to use the existing OPM financial systems. The training team worked with leadership from various OPM program offices to identify the various roles and responsibilities of financial system users. These roles were then mapped to specific job titles and individuals at OPM. The training team met with these users to analyze their competencies, and conducted a gap analysis between the existing skill set and the skills that will be needed to operate CBIS.

The information gathered during this process was formally documented in a deliverable labeled as the "Training/Performance Support Needs Analysis." This deliverable thoroughly outlines the skills that CBIS users will need to receive training on in order to successfully use the various functions of the system.

b. Training Content

The CBIS training team developed three different levels of training content: introductory training which provides an overview of the entire system; detailed overviews of each of the CBIS core process areas; and "hands on" training conducted within a CBIS test environment. The CBIS training curriculum includes a total of 22 courses.

Content for the CBIS training courses was developed with the assistance of Oracle's User Productivity Kit (UPK). Oracle UPK allowed the training team to record screenshots and transactions from the system, annotate them, and replay the content as part of a training course. The training team also developed "job aids" that provide step-by-step instructions for completing a specific transaction within CBIS.

c. Training Delivery

We evaluated the CBIS training team's methodology for ensuring that each CBIS user received the appropriate system training. Each of the 22 CBIS courses is offered in an instructor-led training environment and through the online GoLearn training system.

The CBIS training team's initial task was to identify all CBIS users and determine the level of training that they would require. As mentioned in the "Training Needs" section above, the CBIS training team worked with OPM program offices to identify financial system users and their responsibilities. Based on their understanding of these responsibilities, the training team created a curriculum for each individual CBIS user. The user curriculums were emailed to each user's supervisor, and the supervisor was asked to verify that the training was appropriate for that user.

After the supervisors approved the training for each user, the training team developed a master roster detailing each user's name, position, and each course they were required to complete. This data was then used to generate emails to each individual to notify them of their training requirements.

When an individual has completed all of the training courses in their personal curriculum, the training team notifies the appropriate office that training is complete, and an active CBIS account can be created for that user. Although it has been stressed that CBIS training is required before a user accesses the system, this is currently not an enforceable requirement. The CBIS training team is working with OPM union representatives in an effort to make CBIS training mandatory before user accounts are created. If this is not agreed to, this risk should be mitigated through CBIS' regular risk management process (see the Project Risk Management section discussed below).

The training team uses a combination of sign-in sheets (for instructor led training) and GoLearn's reporting capabilities (for online training) to determine which users have completed a specific training course. The training team currently relies on a manual process to determine when a user has completed all of the required training (by mapping user curriculums to individual course rosters). The weaknesses associated with a manual process increase the risk that a CBIS account could be created for a user that has not completed the appropriate training. However, the CBIS team is aware of this risk and is working with the GoLearn vendor to automate this process.

d. Future Training

Current CBIS training will be permanently available via GoLearn for future users. The training team will continue to develop training courses related to future phases and releases of CBIS. Each training course provides the user with the option of leaving feedback that the training team will consider when developing new courses. The OIG auditors reviewed user feedback for the current courses and found the responses to be generally favorable.

2. Project Risk Management

The OCFO has developed a series of policies and procedures to identify, track, and control risks related to the CBIS system implementation. The OIG interviewed individuals with CBIS risk management responsibility and documented the controls used to manage CBIS project risk. We also collected and reviewed evidence and documentation to evaluate whether these controls are functioning as intended. Although we believe that the OCFO's risk management methodology is very comprehensive, we did detect several anomalies in the process. The following sections outline the results of our risk management review.

a. Background

The OCFO uses a contractor, Booze Allen Hamilton (BAH), to assist in the CBIS risk management process. On a bi-weekly basis, BAH coordinates a meeting with various CBIS stakeholders to review, analyze, discuss, and strategize mitigation options for project risks. Each risk discussed during these meetings is assigned a risk ID number,

and is tracked in a centralized database maintained by BAH. BAH also maintains detailed minute notes for each meeting.

b. New Risks

New project risks can be proposed by any individual involved in the CBIS project. A formal template is used to describe the risk and outline various risk elements such as potential triggers, probability of occurrence, impact, and mitigation technique. Each new risk is discussed at a bi-weekly risk meeting, and the participants agree upon a quantitative value (1-5) for the risk's likelihood of occurrence and potential impact. These two values are combined to determine the risk's initial "score" and subsequent high, medium, or low rating. Each risk is assigned a "risk champion" that is responsible for implementing mitigation activities and providing bi-weekly updates for that risk. BAH is responsible for entering all information about the new risk into the database.

c. Managing Existing Risks

At the bi-weekly risk meetings the participants discuss and analyze each existing risk, beginning with the risks with the highest risk score. The "Top Project Risks" are the 10 risks with the highest score at any given point of time; these risks are the first discussed at every risk meeting. As each risk is addressed, the meeting participants will discuss implemented and potential mitigation techniques, and evaluate whether the value assigned to the various risk elements is still valid. Any updates to the risk's status are documented by BAH and updated in the database.

d. Closing Risks

Risks can be proposed for closure by any participant in the bi-weekly risk meeting. The meeting participants will discuss the reasons a risk is no longer valid, and must all come to an agreement that a risk can be closed. BAH is responsible for documenting the justification for closing each risk and recording this in the database.

Risks can also be closed if the risk event is triggered and becomes an "issue," which is defined as an actual problem that has been observed. When a risk becomes an issue, the CBIS project team develops an "action item" list of steps that must be taken to resolve the issue. Issues and action items are also discussed during the risk management meetings and tracked by BAH in the database.

e. Documentation Review

We requested a listing of the title of every risk in the risk database, a detailed view of the top 10 project risks and previously closed risks, and the meeting minutes from each bi-weekly risk meeting facilitated by BAH. We mapped each of the top 10 project risks to prior meeting minutes (and independently observed one meeting) and concluded that the top risks are being actively discussed and analyzed at the bi-weekly risk meetings.

Although we believe that most risks are discussed and analyzed appropriately, our examination of the meeting minutes and risk inventory database revealed that several risks were closed without adequate documentation or justification. Specifically:

- The risk meeting minutes for January 27, 2009 state that Risk #25 was "retired as of 1/27/09" but no other justification is provided. In addition, this risk could not be located in the inventory.
- Two risks (#40 and #50) are listed as closed in the inventory but no justification for closure is provided. According to the meeting minutes, these risks were most recently discussed on January 27, 2009, where it was documented that there was "No Change."
- Risk #45 is listed as closed in the inventory but no justification for closure is provided. We could not find a record of this risk being discussed in any meeting minutes.
- Risk #47 is listed as closed in the inventory but no justification for closure is provided. According to the meeting minutes, this risk was most recently discussed on November 5, 2008, where the risk probability was increased to medium.

Recommendation 1

We recommend that the CBIS project team implement controls to ensure that documented justification exists to support the closure of each identified risk.

3. Resolution of IV&V Issues

The OCFO contracted with SRA International, Inc. (SRA) to conduct an independent verification and validation (IV&V) of CBIS controls in the requirements and design phases of the system's development. The CBIS project team has a process in place for tracking IV&V findings that they believe require remediation action. However, there is one finding that the IV&V vendor believes requires action whereas the project team does not, and there is no formal process in place to mediate this conflict. The following sections detail our observations related to the IV&V process.

a. IV&V Findings and Project Team Response

SRA was contracted to conduct the IV&V on behalf of OPM's Center for Information Services (CIS), which is responsible for management and oversight of the information technology infrastructure of the agency. The IV&V vendor issued the final IV&V report to the CBIS project team on July 15, 2009 with a total of 10 findings that required remediation action. The CBIS project team issued a response to the IV&V report on July 31, 2009 indicating that they disagreed with all 10 findings or believed that they were out of the intended scope of the review.

The majority of the findings related to documentation or artifacts that the IV&V vendor believed were not provided for review. The OIG auditors met with both the IV&V vendor and the CBIS project team to gain an understanding of each party's position for each of the findings, and to determine what documentation had been provided to the

IV&V vendor. After conducting these meetings, both parties agreed that 9 of the 10 findings required no further remediation action. However, for one finding the IV&V vendor continued to believe that action was required while the CBIS Project team asserted that the item in question was out of the IV&V scope. We found that there is no process in place for resolving disputes of this nature.

b. Tracking IV&V Findings

The CBIS project team developed an IV&V Action Item List to track all findings from the IV&V report. The Action Item List contains the finding title, an assignment of responsibility, a description of the finding, and proposed resolution or action.

Although the CBIS project team acknowledged that the one finding referenced above had not been resolved, this item was listed on the Action Item List with the comment "No CBIS Project action required."

Recommendation 2

We recommend that the senior official with the new Office of Oversight and Compliance determine the appropriate OPM organization and delegate authority for developing and implementing a formal process for mediating disputes involving IV&V reviews.

Recommendation 3

We recommend that the CBIS project team keep all items on the Action Item List open until the IV&V vendor and project team agree upon satisfactory remediation actions.

4. IT Certification and Accreditation

The OCFO contracted with the Enterprise Services Center (ESC) within the Department of Transportation's Federal Aviation Administration to conduct an independent certification and accreditation (C&A) of the IT security controls of CBIS. The C&A was conducted in accordance with OPM's Certification and Accreditation Guide and applicable guidance from the National Institute of Standards and Technology (NIST). The following sections detail our observations related to the CBIS C&A.

a. Information System Security Plan

The completion of an information system security plan (ISSP) is a requirement of OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources. In order to assist agencies in establishing a standardized approach to developing an ISSP, NIST developed SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems.

The ISSP for CBIS was prepared in September 2009 in accordance with the format and methodology outlined in NIST SP 800-18, and contained all major elements suggested by the guidance.

b. Federal Information Processing Standards (FIPS) Publication 199 Analysis

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires the formal categorization of information systems to ensure that the appropriate levels of information security controls are implemented.

NIST SP 800-60 Volume I "Guide for Mapping Types of Information Systems to Security Categories," provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The security categorization analysis for CBIS considered the potential level of impact (*low, moderate, high*) that would result from a loss of confidentiality, integrity, or availability of the system. We determined that this evaluation was compliant with FIPS Publication 199 and NIST requirements, and we agree with the overall security categorization of "moderate" for CBIS.

c. Independent Security Test and Evaluation

A security test and evaluation (ST&E) was completed for the CBIS during September 2009. The ST&E was conducted by ESC, a company independent of OPM and the other contractors supporting CBIS (Accenture and BAH). We verified that the test included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.

ESC evaluated whether the appropriate NIST SP 800-53 security controls were satisfied or not satisfied for CBIS. ESC presented a copy of the evaluation results to the OCFO's office, and helped the program office incorporate the identified weaknesses into the CBIS risk assessment.

d. Risk Assessment

A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

NIST offers a nine step systematic approach to conducting a risk assessment that includes: (1) system characterization; (2) threat identification; (3) vulnerability identification; (4) control analysis; (5) likelihood determination; (6) impact analysis; (7) risk determination; (8) control recommendation; and (9) results documentation.

ESC conducted a risk assessment for CBIS that was based on the guidance of NIST SP 800-30, Risk Management Guide for Information Technology Systems. The CBIS risk assessment was performed in September 2009 and encompassed the nine elements outlined above.

In addition, a privacy impact assessment (PIA) was conducted for CBIS in July 2009. A PIA is used to ensure that no collection, storage, access, use, or dissemination of personally identifiable information occurs that is not needed or authorized. OMB Memorandum M-03-22 outlines the requirements of a PIA. The CBIS PIA was in compliance with OPM's guidance; however, it did not address several requirements applicable to major information systems, including:

- The consequences of collection and flow of information;
- The alternatives to collection and handling as designed;
- The appropriate measures to mitigate risks identified for each alternative; and
- The rationale for the final design choice or business process.

Recommendation 4

We recommend that all of the OMB Memorandum 03-22 requirements are incorporated into the CBIS PIA.

e. Contingency Planning

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

The OCFO has documented contingency plans for CBIS that contain procedures to recover the system following a disruption. Although the CBIS contingency plan contains the majority of critical elements suggested by the NIST guide, we found several discrepancies between two documents critical to the CBIS contingency planning methodology. In addition, we found that the contingency plans did not contain adequate contact information for disaster recovery critical personnel.

The two primary disaster recovery documents for CBIS are: 1) Disaster Recovery Approach, which is Accenture's plan and procedures to recover CBIS when service disruptions occur; and 2) Contingency and Disaster Recovery Plan, which outlines OPM's roles and responsibilities in the disaster recovery process. The discrepancies between these two documents are outlined below:

- The Disaster Recovery (DR) Approach document indicates that it is the Office of Chief Information Office (OCIO)/Chief Information Officer's responsibility to "update the DNS server to resolve to the correct data center when DR is implemented and when the Production environment is restored after DR." However, neither the CBIS Contingency and Disaster Recovery Plan or the OCIO's LAN/WAN disaster recovery plan include instructions on how to perform the DNS server update.

- The Disaster Recovery Approach document indicates that it is OPM's responsibility to coordinate between various disaster recovery planning groups. However, the CBIS Contingency and Disaster Recovery Plan does not address this responsibility.
- The Contingency and Disaster Recovery Plan states that it is Accenture's responsibility to notify users and stakeholders of a system outage or disaster, while the Disaster Recover Approach document indicates that it is OPM's Financial Systems Group responsibility to notify users.
- The Contingency and Disaster Recovery Plan indicates the hot site location is in Cincinnati, Ohio, while the Disaster Recover Approach document states that it is in San Jose, California.
- The Contingency and Disaster Recovery Plan references shipping backup tapes to an off-site Iron Mountain location, while the Disaster Recovery Approach document does not reference the use of off-site backup tapes.

In addition to these discrepancies, we noticed that the CBIS contingency planning documents do not contain detailed contact information for individuals with disaster recovery responsibilities. Although both documents include sections for line of succession and responsibilities as well as personnel contact list, they do not include any information on how to contact these individuals.

Failure to include detailed personnel information or responsibilities in the contingency plan increases the risk that the appropriate personnel will not be notified in the event of a disaster. NIST SP 800-34 states that "Personnel to be notified should be clearly identified in the contact lists appended to the plan. This list should identify personnel by their team position, name, and contact information (e.g., home, work, and pager numbers, e-mail addresses, and home addresses)."

This issue was documented during ESC's security control testing and was included as a finding during that review.

Recommendation 5

We recommend that the OCFO office update the CBIS contingency plans to address the discrepancies outlined in this report and ensure that both documents contain consistent and reliable information and instructions.

f. Plan of Action and Milestones (POA&M)

As part of the C&A Process, ESC provided the OCFO with a POA&M document outlining the security weaknesses detected during the C&A security control testing. All weaknesses and vulnerabilities detected during the C&A process were appropriately included on the CBIS POA&M. Although this POA&M generally adhered to the POA&M format required by OPM's CIS, the weaknesses listed on the CBIS POA&M did not include the following items:

- The individuals assigned responsibility for each weakness;
- The resources required; or

- Proposed completion date.

Once the CBIS POA&M is updated, the document should be used to track security weaknesses identified through any review or audit of the application (e.g., IV&V, OIG audits).

Recommendation 6

We recommend that the OCFO office update the POA&M to identify the individuals assigned responsibility for each weakness, the resources required, or the proposed remediation completion date for each weakness.

5. Overall Testing Strategy

Our review of the overall testing strategy associated with the CBIS project focused on test planning, user acceptance testing, and the defect remediation strategy for any identified problems. Accenture National Security Services is supporting the CBIS testing process.

a. Test Planning

We evaluated the contents of the CBIS project test plan based on the IEEE 829, a recognized standard for software test documentation, and found that the test plan is in substantial compliance with this standard. Only a small number of components included in IEEE 829 are not present in the CBIS test plan. However, these components are present in other testing-related documents.

b. User Acceptance Testing

We interviewed a sample of user acceptance testing (UAT) participants to evaluate Accenture's UAT process. Overall, we found that there were no severe errors encountered during the UAT process and that errors encountered were being handled correctly. Some users indicated that the testing process was positive and that the testing team was very helpful throughout the process. However, we did note several opportunities for improvement from the user perspective:

- Not all users were asked to re-test the functions that failed during the UAT exercise.
- In some cases, UAT participants were frustrated with the script development, lack of accounting knowledge displayed by the Accenture testing team, and the overall UAT process.
- Core UAT personnel (who are also slotted to be trainers) also had concerns about the UAT process. They felt that the test scripts were not very clear and that screen shots would greatly enhance them. They also found that the test scripts were not intuitive; too hard to follow and frustrating; specific to one area (it would have been more helpful to see some processes from end to end.); some scripts were outdated; and a better understanding of the target audience would have resulted in a better script design.

Recommendation 7

We recommend that the CBIS project team improve the user acceptance testing process by considering the user concerns outlined above during future UAT exercises. Specifically, the CBIS team should consider:

- providing better qualified Accenture personnel during the testing sessions, and
- making the scripts user friendly by providing more descriptive information and screen shots of the functions that UAT participants are responsible for testing.

c. Defect Remediation Strategy

The defect management process adopted by the CBIS implementation team appears to be adequate. As of August 19, 2009, 78% of the scripts tested had produced expected results. Unexpected results, which are documented in the form of System Investigation Reports (or SIRs), are being tracked and their resolution is being reported to management and users on a regular basis. There are currently 12 open SIRs, but only one is critical and requires alternative procedures until a modification can be implemented. Overall, none of these unexpected results present a significant risk to the planned October 2009 deployment of CBIS.

If we can be of assistance during your review of this report, please contact me or your staff can contact Michael R. Esser, Assistant Inspector General for Audits, on 606-2143 or Lewis F. Parker, Chief, Information Systems Audits Group, on 606-4738.

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

Richard B. Lowe
Deputy Chief of Staff and Executive Secretariat

Mark Reger
Chief Financial Officer

David M. Cushing
Deputy Chief Financial Officer & Policy and Internal Control Group

[redacted]
Associate CFO
Center for Financial Systems Management

Ronald C. Flom
Associate Director & Chief Human Capital Officer

Matthew E. Perry
Acting Chief Information Officer