Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-15-011

The FDIC's Identity, Credential, and Access Management Program

September 2015

Office of Inspector General

Executive Summary

The FDIC's Identity, Credential, and Access Management Program

Report No. AUD-15-011
September 2015

Why We Did The Audit

Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, issued on August 27, 2004, requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification. As a Government corporation, the FDIC is not subject to HSPD-12. However, the FDIC has decided to voluntarily comply with the goals and objectives of the directive through the Identity, Credential, and Access Management (ICAM) program.

The objectives of the audit were to (1) determine the status of the ICAM program, including progress and costs in relation to goals, budgets, and milestones and (2) identify significant issues or risks that need to be addressed to clarify the long-term direction of the program.

Background

HSPD-12 required the Secretary of Commerce to promulgate, in accordance with applicable law, a federal standard for secure and reliable forms of identification. Following the promulgation, the heads of executive departments and agencies were required, to the maximum extent practicable, to mandate the use of identification by federal employees and contractors that meets the standard in gaining physical access to federally controlled facilities and logical access to federally controlled information systems. Based upon this directive, the National Institute of Standards and Technology developed a standard that includes a description of the minimum requirements for a federal personal identity verification (PIV) card system.

The FDIC awarded a contract (referred to herein as the ICAM contract) in September 2011 to procure expertise and support for the planning and implementation of the ICAM program. Under the terms of the contract, the ICAM program consisted of two phases. The focus of Phase 1 was to issue PIV cards that provide physical access capabilities for FDIC employees and contractor personnel. The focus of Phase 2 was to implement logical access controls using PIV cards (i.e., multi-factor authentication for users of FDIC information systems). Although the FDIC's PIV cards are designed for both physical and logical access, the principal focus of the ICAM program has been on developing and issuing PIV cards for physical access. The FDIC had not funded or prepared a budget for Phase 2 of the ICAM program, and a task order had not been awarded under the ICAM contract for Phase 2 implementation.

Audit Results

Status of the ICAM Program

According to the terms of the ICAM contract, PIV cards should have been issued to all FDIC employees and contractor personnel by August 2014. However, at that time, a significant number of employees and contractor personnel had not received a PIV card. On August 31, 2014, the FDIC executed a contract modification to increase the cost ceiling of the ICAM contract from $3.4 million to $4.9 million. By the close of 2014, the FDIC had expended 90 percent of the ICAM program's total budget.

As of May 1, 2015, only 4,490 of the 8,527 eligible FDIC employees and contractors had been issued PIV cards. On May 11, 2015, the ICAM Executive Committee, which has oversight responsibility for the ICAM program, decided to "pause" the PIV card issuance process until it could adequately reassess the

costs, benefits, and risks of using the General Services Administration's (GSA) USAccess program. At that time, the FDIC was about to proceed with issuing PIV cards to employees and contractor personnel in the FDIC's field offices. On July 3, 2015, the only remaining active task order on the ICAM contract expired. As a result, contractor work on the ICAM program stopped. Responsibility for PIV card rollout activities going forward is being handled by FDIC personnel.

Significant Issues and Risks that Need to be Addressed

As of May 1, 2015, the FDIC had not made a decision about whether to move forward with Phase 2 of the ICAM program. According to officials in the Chief Information Officer (CIO) Organization and the Division of Information Technology (DIT), such a decision would not be made until the FDIC identified an enterprise-wide solution for implementing multi-factor authentication. The decision about whether to use the PIV cards for multi-factor authentication has implications for whether the goals described in the ICAM Project Charter, such as those pertaining to the management of Public Key Infrastructure certificates, can be achieved. Further, if the PIV cards are not used for logical access, they would only provide some marginal additional utility beyond that of the existing FDIC identification badges (i.e., facilitating access to other federal facilities).

Subsequent to the close of our audit field work, the FDIC decided to use USB tokens (rather than PIV cards) for multi-factor authentication. Now that this decision has been made, the FDIC needs to make two additional determinations that impact the long-term direction of the ICAM program. Specifically, the FDIC needs to decide whether all employees and contractors should have PIV cards and, if so, how the Corporation will complete the issuance process. Secondly, the FDIC needs to decide how it will maintain PIV cards and FDIC identification badges going forward. After these determinations are made, the FDIC should focus on:

- clearly defining the roles and responsibilities (including decision-making and accountability) of all parties involved in governing the ICAM program;

- determining the types of cost, budget, performance, and risk reporting that would be effective in measuring whether the ICAM program is meeting established goals and expectations; and

- updating project governance documentation, establishing clear ownership and accountability for ICAM program processes, and making informed and timely decisions.

Like other agencies, the FDIC has been confronted with technical hurdles and challenges in implementing its ICAM program. Other factors have also contributed to delays in fully implementing the ICAM program. Most notably, responsibility for implementing various aspects of the program were divided among two FDIC divisions and there did not appear to be clear ownership or a shared vision of what should be accomplished and how. In addition, the ICAM program was, to some extent, viewed more as an administrative process of issuing PIV cards, rather than the broader program described in the ICAM contract and other ICAM program documentation. Consequently, despite the relatively significant investment in corporate resources involved, the ICAM program was not subject to sufficient and consistently robust governance, which resulted in limited success. In our view, the FDIC's decision to pause the ICAM program for purposes of making critical decisions regarding the program's direction was a prudent one.

Recommendations and Corporation Comments

The report contains two recommendations addressed to the Director, Division of Administration (DOA), to coordinate with the Acting CIO and Director, DIT, to (1) prepare a business case that defines the goals and approach for implementing the ICAM program and (2) establish appropriate governance measures over the ICAM program. The Directors, DOA and DIT, and Acting CIO provided a joint written response, dated September 25, 2015, to a draft of this report. In the response, FDIC management concurred with both recommendations and described planned actions that were responsive.

We identified certain other matters during the audit that we did not consider significant in the context of the audit objectives, and we communicated those separately to appropriate FDIC management officials.

Contents

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, Virginia 22226

Office of Audits and Evaluations
Office of Inspector General

DATE: September 30, 2015

MEMORANDUM TO: Arleas Upton Kea, Director
Division of Administration

Martin D. Henning
Acting Chief Information Officer

Russell G. Pittman, Director
Division of Information Technology

/Signed/
FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Identity, Credential, and Access Management Program* (Report No. AUD-15-011)

Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, issued on August 27, 2004, requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification. As a Government corporation, the FDIC is not subject to HSPD-12. However, the FDIC has decided to voluntarily comply with the goals and objectives of the directive through the Identity, Credential, and Access Management (ICAM) program. This report presents the results of our audit of the ICAM program.

The audit objectives were to (1) determine the status of the ICAM program, including progress and costs in relation to goals, budgets, and milestones, and (2) identify significant issues or risks that need to be addressed to clarify the long-term direction of the program.

To address our objectives, we reviewed relevant status reports, contracting information, and project management documentation. We also interviewed many of those involved in the ICAM program, and evaluated goals, budgets, and milestone information related to the program. We consulted *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide) as a source for sound project management governance practices applicable to initiatives, such as the ICAM program, in conducting our work. We focused our review of the ICAM program on efforts associated with issuing personal identity verification (PIV) cards. In that regard, we performed a walk-through of the FDIC's process for issuing PIV cards to employees and contractor personnel and had several observations. We communicated these observations separately to appropriate

FDIC management officials as the observations were not significant in the context of our audit objectives.

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report includes additional details on our objectives, scope, and methodology. Appendix 2 contains a list of acronyms and abbreviations. Appendix 3 contains the Corporation's comments on this report and Appendix 4 contains a summary of the Corporation's corrective actions.

Background

HSPD-12 was a strategic initiative intended to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 required the Secretary of Commerce to promulgate, in accordance with applicable law, a federal standard for secure and reliable forms of identification. Following the promulgation, the heads of executive departments and agencies were required, to the maximum extent practicable, to mandate the use of identification by federal employees and contractors that meets the standard in gaining physical access to federally controlled facilities and logical access[1] to federally controlled information systems. Based upon this directive, the National Institute of Standards and Technology (NIST) developed a standard that includes a description of the minimum requirements for a federal PIV card system.

OPM Data Breach and the Cybersecurity Sprint

A compromised contractor credential contributed to two recent, highly publicized data breaches at the Office of Personnel Management (OPM). In response to such threats, and to further improve federal cybersecurity, the United States Chief Information Officer (CIO) launched a 30-day Cybersecurity Sprint in June 2015. As part of that effort, the Federal CIO instructed federal agencies to immediately take a number of steps to further protect federal information and assets and improve the resilience of federal networks. Among other things, agencies were to dramatically accelerate implementation of multi-factor authentication, especially for privileged users. According to the Federal CIO, requiring the use of a PIV card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating federal networks and systems.

Federal agencies have experienced mixed success in implementing the requirements of HSPD-12. Challenges to progress have included integrating physical and logical access; testing and acquiring compliant commercial products; ensuring compliance with government-wide requirements and guidance; and establishing effective controls surrounding credentialing contractors.

What Are PIV Cards?

A PIV card contains a microprocessor that stores several electronic identity markers that card holders can use to authenticate their identity in order to gain physical access to

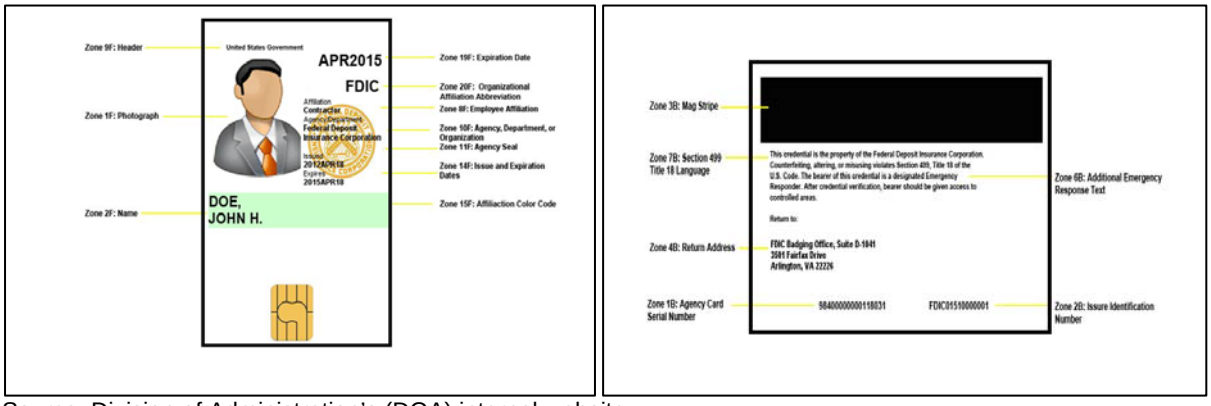
[1] Logical access in information technology (IT) is often defined as interactions with hardware through remote access. This type of access generally features identification, authentication, and authorization protocols. This is often contrasted with the term "physical access," which refers to interactions with hardware in the physical environment, where equipment is stored and used.

federally controlled facilities. A limited amount of personal information is stored on the microprocessor, which includes the following:

- The card holder's name
- Agency affiliation (e.g., the FDIC)
- Two fingerprints
- A personal identification number of the card holder's choosing
- A unique system-generated identifier for the card
- The card expiration date
- An electronic certificate which provides a means for the card holder to electronically identify him/herself

The FDIC PIV card is based on a government-wide federal specification. Figure 1 shows the layout and physical features of both the front and back of the FDIC PIV card.

Figure 1: Illustration of the FDIC PIV Card



Source: Division of Administration's (DOA) internal website.

The FDIC's ICAM Program

The FDIC's ICAM program, which was established in February 2011, is the Corporation's most recent initiative aimed at voluntarily addressing HSPD-12 requirements.[2] According to the ICAM Project Charter, the program was intended to (among other things) define and implement streamlined business processes for (1) identity proofing and registration;[3] (2) background investigations; (3) PIV card

[2] As early as 2006, the FDIC began planning for voluntarily complying with HSPD-12. In the years that followed, the FDIC began upgrading and installing card reader equipment that would be capable of supporting HSPD-12 compliant PIV cards.

[3] Identity proofing is the process of collecting and verifying information about a person for the purpose of proving that a person who has requested an account, a credential, or other special privilege is indeed who he or she claims to be, and establishing a reliable relationship that can be trusted electronically between the individual and credential for purposes of electronic authentication.

issuance, maintenance, and termination; and (4) credential management, including Public Key Infrastructure (PKI) certificates,[4] and physical, and potentially logical, access. In addition, the FDIC envisioned the ICAM program further enhancing the FDIC's security program by improving the chain of trust and by identifying and mitigating any security gaps in processes and/or security systems.

The FDIC awarded a contract (referred to herein as the ICAM contract) in September 2011 to procure expertise and support for the planning and implementation of the ICAM program. After a successful pilot, the FDIC executed a task order in December 2012 to transition to full production and deployment of PIV cards. Both the FDIC's DOA and Division of Information Technology (DIT) have played a role in the ICAM program. The ICAM program began as a joint DIT and DOA initiative. In 2013, the ICAM program budget was transferred from DIT to DOA. Despite this transfer of budget responsibility, the ICAM program has been, and continues to be, managed by a DIT project manager.

The responsibilities of DOA and DIT evolved over the course of the ICAM program. Both DOA and DIT relied on contractor support to carry out many of their respective responsibilities. At the close of our audit, DOA was responsible for handling the administrative aspects of the PIV card issuance process, including handling requests that PIV cards be issued, enrolling PIV card applicants into the Card Management System, verifying background investigations, approving profiles, and printing and issuing PIV cards. Additionally, DOA was responsible for maintaining the Physical Access Control System, which enables physical access to FDIC facilities. DIT, which previously had responsibility for some of the ICAM program activities described above, was responsible for addressing other technical requirements of the program.

Under the terms of the ICAM contract, the ICAM program consisted of two phases. The focus of Phase 1 was to issue PIV cards that provide physical access capabilities to FDIC employees and contractor personnel. The focus of Phase 2 was to implement logical access controls using the PIV cards (i.e., multi-factor authentication for information systems). Although the FDIC's PIV card is designed to be used for both physical and logical access, the principal focus of the ICAM program over the past several years has been on developing and issuing the cards for physical access only. The FDIC had not funded or prepared a budget for Phase 2 of the ICAM program, and a task order had not been awarded under the ICAM contract for Phase 2 implementation.

Project Management Body of Knowledge Guide

The Project Management Institute has conducted extensive research and analysis in the field of project management and published the PMBOK® Guide. The guide documents proven practices, tools, and techniques that have become generally accepted in the field of project management, including information systems development and implementation. The PMBOK® Guide is an approved standard of both the American National Standards

[4] The FDIC's PKI is an agency-wide software tool that provides the FDIC client community with data encryption/decryption and digital signature/verification capabilities.

Institute and the Institute of Electrical and Electronics Engineers. Although the FDIC is not required to comply with the PMBOK® Guide, we used it as criteria because the guide contains generally accepted industry practices for successful project management and the FDIC has incorporated many of the practices into its own project management policies, procedures, and guidance.

Status of the ICAM Program

According to the terms of the ICAM contract, PIV cards should have been issued to all FDIC employees and contractor personnel by August 2014. However, at that time, a significant number of employees and contractor personnel had not received a PIV card. On August 31, 2014, the FDIC executed a contract modification to increase the cost ceiling of the ICAM contract from $3.4 million to $4.9 million. In addition, the FDIC awarded a task order under the ICAM contract on November 3, 2014, to issue PIV cards for employees and contractors in the FDIC's field offices by July 3, 2015. As of May 1, 2015, only 4,490 of the 8,527 eligible FDIC employees and contractors had been issued PIV cards. The table below identifies planned and actual completion dates for key ICAM program milestones.

Table: ICAM Planned and Actual Milestone Dates

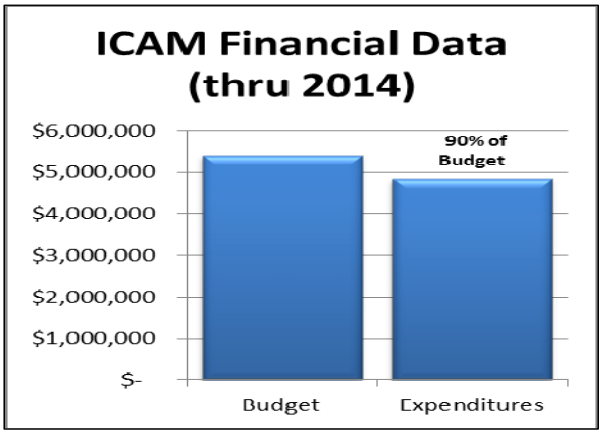
Milestone	Planned Completion Date	Actual Completion Date
Conduct Pilot	2/9/2012	6/30/2012
Assess Pilot	2/29/2012	7/18/2012
Headquarters Deployment	12/31/2013	2/14/2014
Dallas Deployment	12/31/2013	2/14/2014
Atlanta and New York City Deployment	4/28/2014	4/25/2014
Area Office and Remaining Regional Office Deployment	8/29/2014	8/15/2014
Field Office Deployment	8/31/2014	Not Complete
Contractor Deployment	8/31/2014	Not Complete

Source: OIG analysis of ICAM project and executive briefings that occurred between January 2012 and April 2015; the ICAM contract; and information provided by a DIT official.

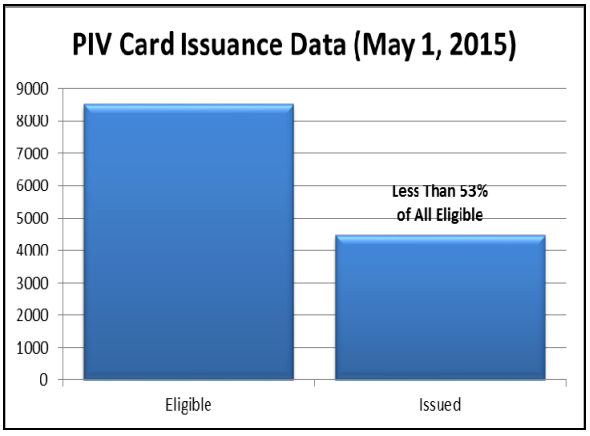
As shown in Figure 2, the FDIC had expended 90 percent of the ICAM program's total budget through 2014. In addition, as of May 1, 2015, the FDIC had issued PIV cards to less than 53 percent of all eligible FDIC employees and contractor personnel. Further, many of the employees and contractors that had been issued PIV cards were allowed to retain their original FDIC identification badges (referred to herein as FDIC ID Badges), which continue to allow access to FDIC facilities. According to the DIT ICAM project manager, the FDIC ID Badges were not collected from employees or contractor personnel when they received their PIV cards because some FDIC card readers were not yet capable of recognizing the PIV card during the initial stages of the PIV card rollout.

The FDIC discontinued its practice of issuing FDIC ID Badges to employees and contractor personnel in July 2015 and now only issues PIV cards.

Figure 2: ICAM Financial and PIV Card Issuance Data



Source: ICAM program briefing, dated January 2015.



Source: ICAM Project Manager.

On May 11, 2015, the ICAM Executive Committee[5] decided to "pause" the PIV card issuance process until it could adequately reassess the costs, benefits, and risks of using the General Services Administration's (GSA) USAccess program.[6] At that time, the FDIC was about to proceed with issuing PIV cards to employees and contractor personnel in the field offices. In our view, the decision to pause the issuance of PIV cards was a prudent one given the significant cost associated with issuing the cards to the field offices—which was estimated to be between $1.2 and $1.5 million.

On July 3, 2015, the only remaining active task order on the ICAM contract expired. As a result, contractor work on the ICAM program stopped. Responsibility for PIV card issuance activities going forward has been assigned to DOA. To assist in the continuation of the ICAM program, DOA plans to contract for subject matter support, as well as background investigations and preliminary screenings. All other PIV card issuance processes will be completed by FDIC personnel.

Significant Issues and Risks that Need to be Addressed

The PMBOK® Guide states that project governance is a critical element of any project. The Guide recommends the assignment of a project manager and team with a structure, including defined roles and responsibilities; processes; decision-making models; and

[5] The ICAM Executive Committee, which consisted of the DIT Director, a DOA Associate Director, and a Senior Counsel in the Legal Division, is responsible for the ICAM program and provides guidance and direction to the project team throughout the program lifecycle.

[6] GSA's USAccess program provides civilian agencies with badging solutions - a nationwide, economical, secure, shared service that facilitates identity credential issuance, maintenance, and lifecycle management. The FDIC assessed the USAccess program prior to the initiation of the ICAM program, but decided not to use the program.

tools for managing the project for successful delivery. Our work identified several issues and risks associated with project governance that contributed to the delays and cost over-runs discussed earlier. These issues and risks warrant priority management attention for purposes of better ensuring the ICAM program meets cost, schedule, and requirements expectations.

Need for Key Decisions on Direction of the ICAM Program

> *The PMBOK® Guide indicates that, as part of scope management, the project team should develop a detailed description of the project and product, including what will be included and excluded from the project scope. The Guide also indicates that effective decision-making involves the ability to negotiate and influence the organization and the project management team. Guidelines for decision-making include: focusing on goals to be served, following a decision-making process, analyzing available information, and managing risk.*
>
> *Further, the ICAM Project Charter includes a critical success factor that states "Executives must make decisions quickly, consistent with the project schedule, and must understand the policy implications and decision points of the new process."*

As of May 1, 2015, the FDIC had not made a decision about whether to move forward with Phase 2 of the ICAM program (i.e., using the PIV cards for logical access to FDIC information systems). According to officials in the CIO Organization and DIT, such a decision would not be made until the FDIC identified an enterprise-wide solution for implementing multi-factor authentication. The decision about whether to use the PIV cards for multi-factor authentication has implications for whether the goals described in the ICAM Project Charter, including those pertaining to PKI certificate management, can be achieved. Further, if the PIV cards are not used for logical access, they would only provide some marginal additional utility beyond that of the existing FDIC ID Badges (i.e., facilitating access to other federal facilities).

Key questions that need to be promptly addressed to clarify the long-term direction of the ICAM program are as follows:

- What is the FDIC's enterprise-wide solution for implementing multi-factor authentication?
    - If the PIV cards will not be used for multi-factor authentication, the FDIC should determine whether it is cost-beneficial to continue issuing PIV cards to the remaining eligible FDIC employees and contractors.
- If the FDIC decides that all employees and contractors should have PIV cards, how will the Corporation complete the issuance process?
    - The FDIC has options to consider, such as utilizing a combination of internal and contractor resources similar to its prior approach, or utilizing a service such as GSA's USAccess program.

- How will the FDIC maintain PIV cards and FDIC ID Badges going forward?

    - PIV cards (including their digital certificates) have a 3-year expiration period. How will maintenance activities, such as renewing cards, replacing lost cards, and maintaining equipment used to generate the cards be handled?
    - How will FDIC ID Badges be maintained and for how long? How will FDIC ID Badges in the possession of PIV card holders be collected and disposed of when they are no longer needed? Having duplicate forms of identification presents additional risk.

Other Steps to Ensure ICAM Program Success

Once the FDIC makes key decisions regarding the direction of the ICAM program (described above), the FDIC should focus on the following areas to ensure successful continuation of its ICAM efforts.

Roles and Responsibilities

> *The PMBOK® Guide states that roles and responsibilities should be clear and documented. Roles and responsibilities include the right to apply project resources, make decisions, sign approvals, accept deliverables, and influence others to carry out the work of the project. Examples of decisions that need clear authority include the selection of a method for completing an activity, quality acceptance, and how to respond to project variances.*

The roles and responsibilities of all parties involved in governing the ICAM program, including decision-making and accountability, had not been clearly defined. In that regard, as we were completing our review, DIT and DOA each performed analyses of certain aspects of the ICAM program.

- On May 8, 2015, DIT produced a *Get Well Plan: ICAM Contractor Enrollment and Issuance*. The plan contained issues and challenges that impacted the contractor PIV card enrollment and issuance process. It also contained corrective actions designed to resolve identified issues.

- On May 12, 2015, DOA's Security and Emergency Preparedness Section performed a review of the ICAM Program that focused on current processes and workload and roles and responsibilities. The review also focused on external elements impacting the ability of the Security and Emergency Preparedness Section to properly perform its functions.

Both the plan and review described above identified risks and issues that illustrated the need to define and/or clarify ICAM program roles and responsibilities and improve coordination and communication among key program stakeholders.

Cost and Performance Management

Cost management involves knowing the financial and human resources required for a project. Project managers should carefully monitor the cost of projects to see where actual cost has varied from estimated cost and inform relevant stakeholders when the variances are significant. Project metrics are used to objectively measure and provide information about the health of a project. They are a source of important data for project control and measuring the project's final deliverable. The PMBOK® Guide also references a performance measurement baseline against which the project execution is compared, and deviations are measured for management control.

The FDIC has produced annual budgets and expense reports for the ICAM program from 2011 through 2014. Through April 30, 2014, the FDIC had spent over $5 million for contractor services, equipment, and federal salaries for the ICAM program. A June 2015 ICAM Executive Briefing identified an estimated $1.73 million budget for 2015. We also obtained a March 2015 CIO Council[7] meeting presentation with client-led IT spending for all FDIC Divisions. In that presentation, DOA had two ICAM line item amounts totaling an additional $3.5 million. This consisted of $925,000 for PIV card enrollment and issuance and $2.6 million for card reader equipment, software, and supplies. These additional related costs were not reflected in the original proposed 2015 ICAM budget. In our view, total ICAM costs, including any maintenance or licensing costs that may occur after the PIV card roll-out, should be aggregated in a comprehensive budget going forward to facilitate management decision-making.

In addition to budget and expense reporting, we observed that risks were identified throughout the ICAM project in steering committee and executive committee briefings. However, the reporting of such information did not appear effective in making it apparent that the project was off-course and in need of re-evaluation and possible re-direction. Accordingly, attention should be focused on determining what type of cost, performance, and risk reporting would be effective in measuring whether the ICAM program is meeting established goals and expectations.

Governance Documents

The PMBOK® Guide states that developing a Project Charter formally authorizes the existence of a project and provides the project manager with the authority to apply organizational resources to project activities. The key benefit of the charter is a well-defined project start and project boundaries, creation of a formal record of the project, and a direct way for senior management to formally accept and commit to the project. In addition, a communication plan is created to indicate agreement on how the team will communicate important information during the project, such as status, meetings, issues, deliverable access, and design/document reviews.

We found that several original ICAM program governance documents did not reflect actual practices. The ICAM Project Charter stated that on February 22, 2011, the CIO

[7] The CIO Council advises the CIO on all aspects of the adoption and use of IT at the FDIC and has sole authority to review and approve all ICAM program-related funding requests.

Council approved the ICAM program. However, the ICAM program was actually approved to go forward by DIT's Project Initiation Review Committee on February 16, 2011.[8] In addition, the charter stated that the CIO Council provides a leadership forum and governance structure for discussing issues of mutual interest across organizational boundaries. The ICAM Communication Plan, which was electronically linked to the ICAM program charter, also indicated that in the event that the ICAM Executive Committee could not reach a consensus, the matter in question would be elevated to the CIO Council. However, we determined that the CIO Council had not played any role in ICAM program governance. The charter also named certain senior FDIC personnel who were not involved in the ICAM program.

Further, we found that DIT's Program Management Office[9] developed ICAM PIV Issuance Plans that included contractor-specific activities. Now that the ICAM contract has expired, all PIV card issuance processes and activities are being performed by FDIC personnel. Accordingly, the project plans will need to be updated.

The ICAM Project Charter was updated as of April 2015 to (among other things) re-define the ICAM governance structure as the ICAM Executive Committee, Steering Committee, and Working Group.[10] These governing bodies have met periodically during the life of the ICAM program and the frequency of the Executive Committee meetings increased in 2015. However, continued attention is needed to ensure that:
(1) inaccuracies in the initial Project Charter and communication plan are addressed;
(2) ownership and accountability for ICAM program processes are clearly defined; and
(3) decision-making is informed and timely. Changes will also need to be incorporated into the governance documents to reflect critical decisions the FDIC makes regarding future deployment and possible expanded use of the PIV card, and any related new strategies and approaches for fully implementing the ICAM program.

Conclusions and Recommendations

The FDIC has been working towards implementing PIV cards since 2006, with the most recent initiative being the initiation of the ICAM program in 2011. Overall, the Corporation's efforts have resulted in limited success. Like other agencies, the FDIC has been confronted with technical hurdles and challenges. Other factors have also contributed to delays in fully implementing the ICAM program. Most notably, responsibility for implementing various aspects of the program have been divided among

[8] The Project Initiation Review Committee is DIT's governing body for determining project viability. The Committee is comprised of all DIT Deputy Directors. The major objectives of the Committee's review of a proposed project are for the DIT Deputies to be aware of and understand the project's scope (i.e., resources, staffing, time, and budget) by performing a high-level review of the proposed project and to approve, disapprove, or modify the project scope that is presented.
[9] The Program Management Office is responsible for maintaining and enhancing the FDIC's system development life cycle methodology (SDLC) and providing assistance to IT development teams on the use and tailoring of the SDLC for execution of the team's IT development efforts.
[10] The Working Group members provide expertise in their respective business areas to support the program activities and assist in establishing clear communication between the stakeholders and their organization.

two divisions and there did not appear to be clear ownership or a shared vision of what should be accomplished and how. In addition, the ICAM program was, to some extent, viewed more as an administrative process of issuing PIV cards rather than the broader program described in the ICAM contract and other program documentation. Consequently, despite the relatively significant investment in corporate resources involved, the ICAM program was not subject to sufficient and consistently robust governance.

As noted earlier in our report, the FDIC has wisely paused the ICAM program for purposes of re-evaluation and to make critical decisions regarding its direction. In addition, recent emphasis by the Federal CIO on implementing multi-factor authentication underscores the importance of adopting an enterprise-wide multi-factor authentication solution that will impact the future direction of the ICAM program.

We are making two recommendations that are intended to assist FDIC management in its re-evaluation of the ICAM program and ensure that governance measures are put in place to better monitor progress and ensure the program's success.

Recommendations

We recommend that the Director, DOA, in coordination with the Acting CIO and Director, DIT:

(1) Prepare a business case that defines the FDIC's goals and approach for implementing the ICAM program. The business case should reflect consideration of relevant costs, benefits, risks and options, as well as, the FDIC's decision regarding an enterprise-wide multi-factor authentication solution.

(2) Based on the business case developed in recommendation 1:

a) Establish and revise, as appropriate, the roles and responsibilities (including decision-making and accountability) of key parties involved in implementing and overseeing the ICAM program.

b) Prepare or update, as appropriate, all ICAM governance documentation to reflect the revised project and governance structure. Such documentation should include, among other things:

- a project charter;
- a communication plan;
- project plan(s);
- a comprehensive budget that includes all foreseeable costs including, but not limited to, contractor services, current and future maintenance costs, FDIC salaries, and equipment; and
- performance measures and reporting.

Corporation Comments and OIG Evaluation

After we issued our draft report, management provided us with technical comments for our consideration, and we revised our report to address those comments, as appropriate. The Director, DOA, Acting CIO, and Director, DIT, provided a joint written response, dated September 25, 2015, to a draft of this report. The response is provided in its entirety in Appendix 3. In the response, FDIC management concurred with both recommendations. A summary of the Corporation's corrective actions is presented in Appendix 4. The planned actions are responsive to the recommendations and the recommendations are resolved.

Objectives, Scope, and Methodology

Objectives

The audit objectives were to (1) determine the status of the ICAM program, including progress and costs in relation to goals, budgets, and milestones, and (2) identify significant issues or risks that need to be addressed to clarify the long-term direction of the program.

We conducted this performance audit from January 2015 through August 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

The audit focused on ICAM program activities that occurred during the period February 2011 through August 2015. We also became familiar with the FDIC's HSPD-12 related activities prior to that time period to ensure proper context when presenting our results.

To obtain an understanding of the FDIC's ICAM program, we reviewed:

- HSPD-12;
- NIST Federal Information Processing Standards Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;
- ICAM program governance documents, such as the ICAM project charter, communication plan, and implementation road map; and
- relevant FDIC policies, procedures, and guidance.

To address our objectives, we reviewed:

- the ICAM contract and related task orders;
- project management documentation and analyses prepared by DIT and DOA, including ICAM Executive Committee and ICAM Steering Committee meeting minutes and briefings, as well as communication and project plans; and
- project expense and budget information obtained from FDIC officials and system-generated reports.

Objectives, Scope, and Methodology

We also spoke with officials in DOA, DIT, and the CIO Organization about the risks, goals, status, challenges, costs, schedule, and decision-making related to the ICAM program. We consulted the PMBOK® Guide as a source for sound project management governance practices applicable to initiatives, such as the ICAM program, in conducting our work.

We focused our review of the ICAM program on the FDIC's efforts to issue PIV cards because the principal focus of the ICAM program over the past several years has been on developing and issuing PIV cards for physical access only. The FDIC had not funded or prepared a budget for Phase 2 of the ICAM program, and a task order had not been awarded under the ICAM contract for Phase 2 implementation. We performed walk-throughs of the FDIC's process for issuing PIV cards to employees and contractor personnel in May 2015. We developed several observations during these walk-throughs that we communicated separately to appropriate FDIC management officials as the observations were not significant in the context of our audit objectives.

We obtained and analyzed cost and expense information from the FDIC's core financial system known as the New Financial Environment as well as contract documentation from the FDIC's Contract Electronic File. We did not perform audit procedures to assess information system controls associated with this information because such procedures were not necessary to accomplish our audit objectives. Rather, we corroborated the reliability of automated information as appropriate through discussions with FDIC management officials and our review of other relevant documentation. In addition, we did not assess the FDIC's compliance with laws and regulations because doing so was not necessary to accomplish our audit objectives. Further, we assessed the risk of fraud and abuse related to our audit objectives in the course of evaluating audit evidence.

We conducted our work at the FDIC's Virginia Square offices in Arlington, VA.

Appendix 2

Acronyms and Abbreviations

CIO	Chief Information Officer
DIT	Division of Information Technology
DOA	Division of Administration
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
ICAM	Identity Credential and Access Management
ID	Identification
IT	Information Technology
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMBOK®	Project Management Body of Knowledge
SDLC	System Development Life Cycle

Corporation Comments

Federal Deposit Insurance Corporation
3501Fairfax Drive, Arlington, VA 22226

DATE: September 25, 2015

MEMORANDUM TO: Mark F. Mulholland
Assistant Inspector General for Audits

FROM: Arleas Upton Kea, Director /**Signed**/
Division of Administration

Martin D. Henning /**Signed**/
Acting Chief Information Officer

Russell Pittman, Director /**Signed**/
Division of Information Technology

SUBJECT: Management Response to the Office of Inspector General Draft Audit Report Entitled, *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (Assignment No. 2015-016)

The Division of Administration (DOA) and the Division of Information Technology (DIT) have reviewed the subject draft audit report dated August 26, 2015. We agree with the findings and recommendations and have provided timelines for corrective action below.

The report states that the ICAM program has lacked clear ownership and a shared vision of what should be accomplished and how, and we agree. This project required a strong partnership and clear responsibilities between DOA and DIT, and close coordination with the remaining divisions and offices. These characteristics were especially critical given the technical issues the FDIC and many other government agencies have faced in attempting to implement Personal Identity Verification (PIV) card solutions (for example integrating physical and logical access; testing and acquiring compliant commercial products; evolving government-wide guidance; and establishing effective controls around credentialing contractors). The partnership and clear delineation of responsibilities has not been as strong as needed and we are already addressing this deficiency.

The report also states that the program was viewed as an administrative program that did not require consistently robust governance, and we agree. The FDIC is committed to protecting personal privacy, enhancing security, and reducing identity fraud. We will re-focus on the ICAM program and provide appropriate governance to ensure that it meets relevant federal standards.

As we have worked with the auditors and learned of deficiencies, we have begun to take action to correct issues discovered. For example, we re-constituted an executive governance committee to assess where the program stands, what actions are necessary to finish the PIV card deployment

Corporation Comments

in all locations other than field offices (where the deployment has been paused), and to consider options for further multi-factor authentication implementation. The committee is comprised of the Director of DOA, the Director of DIT, the Acting Chief Information Officer, the Chief Information Security Officer, and the Deputy Director of DOA's Corporate Services Branch who oversees physical security. The committee first met on June 3, 2015 and has met three times since then. The ICAM charter is being revised through this group, and several actions have been taken to ensure the current PIV card deployment and maintenance is stabilized. We have also made a decision on the multi-factor authentication solution that will be deployed and are beginning the implementation. Further actions we will take that are directly responsive to the report recommendations are provided below.

Recommendation 1: Recommend that the Director of DOA, in coordination with the Acting CIO and Director, DIT prepare a business case that defines the FDIC's goals and approach for implementing the ICAM program. The business case should reflect consideration of relevant costs, benefits, risks and options, as well as, the FDIC's decision regarding an enterprise-wide multi-factor authentication solution.

Management Response: Management concurs with this recommendation.

Corrective Action: DOA will partner with DIT and the Acting CIO to prepare a business case that defines the FDIC's goals and approach for completing the ICAM program including using multi-factor authentication. The business case will reflect our consideration of relevant costs, benefits, risks, and options.

Recently, management has decided to use USB tokens for multi-factor authentication for non-privileged and non-remote users. We are moving forward with full implementation of the USB tokens and anticipate completion by the end of the second quarter 2016. In addition to our business case addressing the goals and approach for the ICAM program, the case will convey the basis for using USB tokens for multi-factor authentication.

Completion Date: The business case will be completed by January 31, 2016.

Recommendation 2: Based on the business case developed in recommendation 1: Recommend that the Director of DOA, in coordination with the Acting CIO and Director, DIT do the following:

A) Establish and revise, as appropriate, the roles and responsibilities (including decision making and accountability) of key parties involved in implementing and overseeing the ICAM program.

[1] Multi-factor authentication has been implemented for remote access for many years, and for privileged users for approximately one year. The next implementation will be for network access from within FDIC facilities.

Corporation Comments

B) Prepare or update, as appropriate, all ICAM governance documentation to reflect the revised project and governance structure. Such documentation should include, among other things:
   - A project charter;
   - A communication plan;
   - Project plan(s);
   - A comprehensive budget that includes all foreseeable costs including, but not limited to, all contractor services, current and future maintenance costs, FDIC salaries, and equipment; and
   - Performance measures and reporting.

Management Response: Management concurs with this recommendation.

Corrective Action: DOA will partner with DIT and the Acting CIO to:

- Roles and Responsibilities: Establish and revise, as appropriate, the roles and responsibilities of key parties involved in implementing and overseeing the ICAM program.
- Project Charter: Update the Project Charter to clearly specify the operational authority, funding authority, and oversight authority.
- Communication Plan: Prepare a comprehensive communication plan to help formalize information sharing with key stakeholders and agency officials.
- Project Plan: Update the ICAM project plan to address items mentioned throughout the OIG's report.
- Budget Plan: Prepare a new comprehensive budget plan that will include all foreseeable costs including contractor services, current and future maintenance costs, FDIC salaries, and equipment. A review of existing budget plans will be conducted to reflect the new oversight and management of the program within DOA.
- Performance Measures: Identify and document specific metrics that will be used to measure and report the status of ongoing project goals and accomplishments.
- ICAM Policy: Develop an FDIC ICAM policy/directive outlining the program structure, roles and responsibilities comparable to other FDIC security program policies; i.e. physical security, personnel security, etc. The policy will identify the management roles and responsibilities of the stakeholder entities having operational management over different facets of ICAM, i.e. DOA, DIT, and CISO and define specific roles in the PIV process that need to be maintained to ensure compliance with FIPS, NIST and HSPD-12, i.e. separation of roles.

An executive committee has been meeting and coordinating actions since June re-establish the strategic direction for the program, implement better tracking mechanisms, and to make changes to the governance structure. This report will inform those efforts already underway.

Completion Date: January 31, 2016

Questions regarding this response should be directed to Dan Bendler 703-562-2123.

Corporation Comments

cc: Barbara A. Ryan, Deputy to the Chairman and Chief Operating Officer
Steven O. App, Deputy to the Chairman and Chief Financial Officer
Elaine Stankiewicz, Senior Advisor, Deputy to the Chairman and CFO
Ronald T. Bell, Deputy Director, DOA, Corporate Services Branch
Daniel H. Bendler, Assistant Director, DOA, Management Services Branch
Rack Campbell, Supervisory IT Specialist, DIT, AICS

Summary of the Corporation's Corrective Actions

This table presents corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or[b] Closed
1	DOA will partner with DIT and the Acting CIO to prepare a business case that defines the FDIC's goals and approach for completing the ICAM program. The business case will reflect consideration of relevant costs, benefits, risks, and options as well as the basis for using USB tokens for multi-factor authentication for non-privileged and non-remote users.	1/31/2016	No	Yes	Open
2	DOA will partner with DIT and the Acting CIO to establish and revise, as appropriate, the roles and responsibilities of key parties involved in implementing and overseeing the ICAM program. In addition, the following items will be updated: the Project Charter, Communication Plan, Project Plan and Budget Plan. Further, specific metrics will be identified and documented and an ICAM policy/directive will be developed.	1/31/2016	No	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.