Office of Inspector General

Office of Information Technology Audits and Cyber
Report No. AUD-17-004

Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program

June 2017

Office of Inspector General

Executive Summary

Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program

Report No. AUD-17-004
June 2017

Why We Did The Audit

On September 30, 2015, we issued an audit report, entitled *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (the ICAM Audit Report). The FDIC established the ICAM program in February 2011 to address the goals and objectives of Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. HSPD-12 requires (among other things) that executive departments and agencies implement a government-wide standard for secure and reliable forms of identification that allow employees and contractor personnel to access federally-controlled facilities and information systems. The ICAM Audit Report indicated that the FDIC had not achieved its goal of issuing identity credentials (known as personal identity verification (PIV) cards) to all eligible employees and contractor personnel. In addition, the FDIC had not established appropriate governance to ensure the ICAM program's success. The ICAM Audit Report included recommendations for the FDIC to define the goals and approach for implementing the program and to establish appropriate governance.

In light of the concerns raised in the ICAM Audit Report, the Chairman of the FDIC Audit Committee requested that we conduct follow-up audit work related to the ICAM program. We also determined that follow-on work in this area was warranted. The objective of this audit was to assess the FDIC's plans and actions to address the recommendations contained in the ICAM Audit Report.

Background

The FDIC awarded a contract in September 2011 to procure expertise and support for planning and implementing the ICAM program. According to ICAM program documentation, the FDIC intended to use PIV cards to control access to both FDIC facilities and the Corporate network. The FDIC used a commercially-available PIV card management solution to issue and maintain PIV cards. More than 4 years after the ICAM program was initiated, only half of the FDIC's employees and contractor personnel had a PIV card, and steps had not been taken toward using the cards to access the Corporate network. In May 2015, the FDIC decided to temporarily suspend issuance of new PIV cards under the ICAM program. The FDIC wanted to assess the costs, benefits, and risks of using an alternative solution—the General Services Administration's USAccess program. The USAccess program is a government-wide service that federal agencies can use to provide their employees and contractor personnel with PIV cards.

In November 2015, the FDIC hired a new Chief Information Officer (CIO) who subsequently decided to reorganize and incorporate the ICAM program into a new enterprise-wide program, the Access Control Program (ACP). The objectives of this new ACP were to comply with HSPD-12 and consolidate the FDIC's identity management and access control-related projects into a single program. The CIO also decided that PIV cards would be used to gain access to the Corporate network and that the cards would be issued and maintained using the USAccess program, rather than the FDIC's legacy PIV card system.

Audit Results

We reviewed the actions taken by the Corporation to address the recommendations in our ICAM Audit Report issued in September 2015 and closed the recommendations. Notwithstanding our decision to close the recommendations, we found that the FDIC experienced considerable challenges and that there were risks warranting management's attention as the Corporation issued PIV cards to its employees and

contractor personnel and enabled the cards to support access to the Corporate network. The FDIC took steps to address those challenges and risks during our audit. However, our report identifies the following three aspects of the program that still need improvement.

- The FDIC had not established corporate policies and procedures governing the management and use of PIV cards for physical and logical access. Such policies and procedures are important for ensuring that employees and contractor personnel become aware of, and fully understand and properly carry out, their responsibilities with respect to PIV cards.

- The FDIC did not maintain current, accurate, and complete contractor personnel data needed to manage PIV cards. Absent reliable contractor personnel data, PIV cards may not be issued and revoked in a timely manner, presenting an increased risk of unauthorized access to FDIC facilities and the Corporate network.

- FDIC management had not finalized and approved a plan for retiring the FDIC's legacy PIV card system. Without such a plan, the FDIC may incur unnecessary costs associated with maintaining the system longer than needed, and sensitive information in the system may not be disposed of in a timely or safe manner.

Recommendations and Corporation Comments

The report contains four recommendations addressed to the FDIC CIO and the Directors, Division of Administration and Division of Information Technology, that are intended to strengthen internal controls over the issuance and maintenance of PIV cards used to access FDIC facilities and the Corporate network. In a written response to a draft of this report, FDIC management concurred with our recommendations and described planned and completed actions that were responsive.

Contents

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

Office of Information Technology Audits and Cyber
Office of Inspector General

DATE: June 8, 2017

MEMORANDUM TO: Arleas Upton Kea, Director
Division of Administration

Lawrence Gross, Jr.
Chief Information Officer

Russell G. Pittman, Director
Division of Information Technology

/Signed/
FROM: Mark F. Mulholland
Assistant Inspector General for
Information Technology Audits and Cyber

SUBJECT: *Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program*
(Report No. AUD-17-004)

On August 27, 2004, the President issued Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*.[1] HSPD-12 stated that wide variations existed in the quality and security of identification forms used to gain access to federally-controlled and other facilities where the potential for terrorist attacks exist. To eliminate these variations, HSPD-12 required the development of a government-wide standard for secure and reliable forms of identification that executive departments and agencies must follow when issuing identification to their employees and contractor personnel. HSPD-12 directed executive departments and agencies, to the maximum extent practicable, to require the use of such identification for physical access to federally-controlled facilities and logical access to federally-controlled information systems.[2] Many federal agencies address this requirement by providing their employees and contractor personnel with an identity credential called a personal identity verification (PIV) card.

[1] It is the FDIC's position that HSPD-12 is not binding on the Corporation. This position is consistent with the Office of Management and Budget's (OMB) Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors,* dated August 5, 2005, which states that government corporations are encouraged, but not required, to implement HSPD-12. Nevertheless, the FDIC has chosen to voluntarily address with the goals and objectives of HSPD-12.

[2] Physical access refers to the entry and exit by individuals into or out of physical areas, such as buildings. Logical access refers to accessing electronic information and/or computer systems.

On September 30, 2015, we issued an audit report, entitled *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (the ICAM Audit Report).[3] The report focused on the FDIC's efforts to issue PIV cards to its employees and contractor personnel and to identify and implement a corporate-wide multifactor authentication (MFA) solution.[4] In the report, we found that the FDIC had not achieved its goal of issuing PIV cards to all eligible employees and contractor personnel. In addition, the FDIC had not defined clear roles and responsibilities, ownership, accountability, or governance over the ICAM program.

The ICAM Audit Report made two recommendations for the FDIC to (1) prepare a business case that defines the goals and approach for implementing the ICAM program and (2) establish and revise, as appropriate, the roles and responsibilities of key parties and prepare or update, as appropriate, all ICAM governance documentation. In light of the concerns raised in the ICAM Audit Report, the Chairman of the FDIC Audit Committee requested that we conduct follow-on audit work related to the ICAM program. We also determined that follow-on work in this area was warranted.

The objective of this audit was to assess the FDIC's plans and actions to address the recommendations contained in the ICAM Audit Report. To achieve the audit objective, we reviewed the FDIC's plans and actions to determine whether they were responsive to the recommendations; interviewed FDIC staff who had responsibility for developing and implementing the plans and actions; and attended management meetings where project goals, risks, budgets, and status were discussed. We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report includes additional details about our objective, scope, and methodology; Appendix 2 contains a list of acronyms and abbreviations; Appendix 3 contains the Corporation's comments; and Appendix 4 contains a summary of the Corporation's corrective actions.

Background

On February 25, 2005, in response to HSPD-12, the Secretary of Commerce issued Federal Information Processing Standards Publication (FIPS PUB) 201, entitled *Personal Identity Verification of Federal Employees and Contractors*. FIPS PUB 201 defined the minimum requirements for a federal PIV card system based on secure and reliable forms

What is a PIV Card?

A PIV card is a hand-carried identity credential issued by a federal government entity. A PIV card contains a computer chip with data that allows the cardholder to be granted access to federally-controlled facilities and information systems.

[3] The report can be found at https://www.fdicig.gov/reports15/15-011AUD.pdf.
[4] MFA is a method of verifying the identity of an individual seeking access to an information system. MFA uses a combination of factors, such as passwords, PIV cards, or tokens, to verify an individual's identity.

of identity credentials issued by the federal government to its employees and contractor personnel. In August 2013, the Secretary of Commerce reissued the publication as FIPS PUB 201-2 under the same title to address such things as technological advancements that had occurred since the original publication and to clarify ambiguities in the original text.[5]

The National Institute of Standards and Technology (NIST), an agency within the Department of Commerce, recommends that federal agencies implement MFA to control logical access to their moderate- and high-impact information systems.[6] According to NIST, MFA makes it more difficult for an attacker to gain unauthorized access to an information system than single factor authentication because the attacker must compromise two factors—not just one—to gain access.

In June 2015, the U.S. Chief Information Officer (CIO) launched a government-wide initiative known as the "30-day Cybersecurity Sprint" to improve federal cybersecurity and protect information systems against evolving threats.[7] As part of this initiative, the U.S. CIO instructed federal agencies to take a series of steps to further protect their information and assets and improve the resilience of their networks. One such step was to "dramatically accelerate implementation of multi-factor authentication, especially for privileged users."[8] The U.S. CIO added "intruders can easily steal or guess usernames and passwords and use them to gain authorized access to federal networks, systems, and data. Requiring the utilization of a Personal Identity Verification (PIV) card or alternative forms of multi-factor authentication can significantly reduce this risk of adversaries penetrating federal networks and systems."

On October 30, 2015, OMB issued guidance to executive departments and agencies through its Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*. OMB Memorandum M-16-04 stated, among other things, that using PIV cards to support identity verification and authentication to federal

[5] It is the FDIC's position that FIPS 201-2 is not binding on the Corporation because the publication was issued by the Secretary of Commerce who, under Title 40 of the United States Code in effect in 2013, generally does not have jurisdiction over the FDIC. Nevertheless, the FDIC has chosen to voluntarily comply with the goals and objectives of FIPS 201-2.

[6] See NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013. It is the FDIC's position that NIST SPs contain statements of best practices or guidance and are not binding on the Corporation. NIST SP 800-53, Revision 4, together with NIST FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004, define a framework for categorizing information systems as high, moderate, or low based on the potential impact of a system's loss of confidentiality, integrity, or availability. It is the FDIC's position that FIPS PUB 199 is not binding on the Corporation, but the FDIC has adopted it as policy.

[7] See OMB's *FACTSHEET: Enhancing and Strengthening the Federal Government's Cybersecurity*, dated June 17, 2015. The U.S. CIO leads the Office of Electronic Government and Information Technology (IT) within OMB. The U.S. CIO is responsible for providing leadership regarding electronic government, overseeing federal IT spending, and working with OMB management regarding policy and strategic planning of federal IT investments.

[8] Privileged users include, for example, IT administrators who have elevated access rights that allow them to bypass security and other controls to perform necessary maintenance and troubleshooting.

information resources is a "cost-effective and immediate action that agencies should take to drastically reduce their risk profiles."[9]

The FDIC's Efforts to Implement HSPD-12

In February 2011, the FDIC initiated its ICAM program to address the goals and objectives of HSPD-12. The ICAM program followed previous efforts by the FDIC to address the intent of HSPD-12 that began as early as 2006.[10] In September 2011, the FDIC awarded a contract to procure expertise and support for planning and implementing the ICAM program. Under the terms of the contract, PIV cards were to be issued to all eligible FDIC employees and contractor personnel by the end of 2014. The FDIC used a commercially-available PIV card management solution to support PIV card issuance and maintenance. Although the ICAM program was intended to address both physical and logical access, the program focused on developing and issuing PIV cards for physical access only. The FDIC's Division of Administration (DOA) and Division of Information Technology (DIT) shared responsibility for managing the ICAM program.

In early 2015, more than 4 years after it was initiated, the ICAM program had achieved limited success. As of May 1, 2015, the FDIC had issued PIV cards to only 53 percent of its eligible employees and contractor personnel. In addition, the FDIC had not taken steps toward using PIV cards for logical access. At that time, the FDIC was about to issue PIV cards to employees and contractor personnel in the FDIC's 82 field office locations. FDIC personnel recognized that doing so presented logistical challenges because the field offices were geographically dispersed around the country.

On May 11, 2015, the FDIC decided to suspend the issuance of new PIV cards. The FDIC wanted to assess the costs, benefits, and risks of using an alternative solution—the General Services Administration's (GSA) USAccess program. GSA established the USAccess program as a government-wide service that federal agencies can use to provide their employees and contractor personnel with PIV cards. The USAccess program was a potentially viable alternative to the ICAM program at the FDIC. The USAccess program had several hundred locations around the country where PIV cards could be obtained. The FDIC ultimately decided to use the USAccess program as the Corporation's PIV card management solution.

The ICAM Audit Report

In our September 2015 ICAM Audit Report, we concluded that despite a relatively significant investment of corporate resources, the ICAM program resulted in limited success. The report indicated that responsibility for implementing the program was

[9] It is the FDIC's position that OMB Memorandum M-16-04 is generally applicable to the Corporation and that it would be prudent to comply with the memorandum's provisions regarding the use of PIV cards for MFA to secure information resources.

[10] Such previous efforts included upgrading and installing card reader equipment in FDIC facilities that would be capable of supporting HSPD-12 compliant PIV cards.

divided between two FDIC divisions and that there was no clear ownership or a shared vision of what should be accomplished and how. In addition, the earlier ICAM program was not subject to sufficient governance. The ICAM Audit Report contained two recommendations addressed to the Director, DOA, to coordinate with the then-Acting CIO and Director, DIT, to:

(1) Prepare a business case that defined the FDIC's goals and approach for implementing the ICAM program. The business case was to reflect consideration of relevant costs, benefits, risks, and options, as well as the FDIC's decision regarding an enterprise-wide MFA 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.

FDIC management concurred with both recommendations and described responsive actions that would be completed by January 31, 2016. As discussed next, FDIC management subsequently advised us that the FDIC had decided to pursue a different approach to address the recommendations related to the ICAM program.

The FDIC's Revised Approach to Address the ICAM Audit Report Recommendations

In November 2015, the FDIC hired a new CIO who subsequently decided to reorganize and incorporate the ICAM program into a new enterprise-wide Access Control Program (ACP). The objectives of the ACP were to comply with HSPD-12 and FIPS 201-2, and to consolidate the FDIC's identity management and access control-related projects into a single program.[11] The ACP was intended to improve coordination and integration among these projects and ensure they shared a common vision. The CIO also decided that PIV cards would be used to support logical access to the Corporate network and that the cards would be issued and maintained by the USAccess program, rather than the FDIC's legacy PIV card system. This approach represented a departure from management's original response to our ICAM Audit Report indicating that Universal Serial Bus (USB) tokens would be used to support logical access for all employees and contractors. This change in approach resulted in some inefficiencies, as the FDIC did not use the tokens it had

[11] Other projects consolidated into the ACP include, for example, an initiative to replace the FDIC's existing system used to manage access to Corporate information systems and resources and an initiative to automate existing processes that support the hiring and departure of FDIC personnel.

purchased for their intended purpose, and additional time and resources were required to plan and implement the new approach.[12]

In a memorandum to our office dated February 29, 2016, FDIC management explained that using PIV cards to support logical access and establishing the ACP was consistent with OMB policy and the FDIC CIO Organization's broader strategy of consolidating the management and coordination of identity management and access control activities. The table below summarizes the revised corrective actions that the FDIC committed to take to address the ICAM Audit Report recommendations.

Table: Summary of Management's Revised Corrective Actions

Recommendation Number	Revised Corrective Actions	Planned Completion Date
1	The FDIC will develop and finalize the following documents that will reflect the change in strategic direction to use PIV cards. ACP Business Case ACP Communication Plan ACP Performance Measures ACP Program Charter ACP Policy Statement	April 29, 2016
2	After obtaining funding and making arrangements to use the USAccess program, the FDIC will develop and finalize: (1) an ACP Program Plan that addresses the deployment of PIV cards and the roles and responsibilities of key parties and (2) budget plans.	June 30, 2016

Source: Office of Inspector General (OIG) review of the FDIC's revised approach to address the ICAM Audit Report recommendations as described in management's February 29, 2016 memorandum to our office.

We reviewed the information provided by the Corporation intended to address the revised corrective actions and determined that the information addressed the concerns that prompted our original recommendations. Accordingly, we closed the recommendations.

Notwithstanding our decision to close the recommendations, the FDIC experienced considerable challenges and risks as it worked to issue PIV cards to its employees and contractor personnel and enable the cards to support logical access to the Corporate network. The following sections of the report describe these challenges and risks and how management has addressed them, and identifies aspects of the program that still need improvement.

[12] The FDIC extended the timeframe for completing the implementation of MFA from the second quarter of 2016 to fourth quarter of 2016.

Risks Regarding Project Governance

On April 27, 2016, we informed FDIC management that although steps had been taken to strengthen governance over its PIV card management and MFA activities, significant risks and issues remained that warranted management's attention. Specifically:

- The CIO Organization and DOA were expending considerable resources to issue PIV cards and develop an MFA solution without written implementation plans, approved budgets, or regular expenditure reporting to executive management.

- The level of resources committed to issuing and maintaining PIV cards was not commensurate with the workload in this area.

- The FDIC did not maintain a reliable source of personnel information for contractors that could be used to support the PIV card issuance process.

- The CIO Organization and DOA had not developed a strategy to communicate the FDIC's plans and approach, as well as the responsibilities and expectations of employees and contractor personnel, regarding the use of PIV cards for physical and logical access.

The FDIC subsequently took actions to mitigate these risks during our current audit. For example, the FDIC developed project and budget plans and began reporting expenditure information to executive management; increased the level of resources dedicated to PIV card management; and developed and implemented a written communications strategy.

Notwithstanding these actions, the FDIC still needed to establish corporate policies and procedures to govern its PIV card management and MFA activities; take steps to ensure that contractor data used to support PIV card issuance and maintenance remains reliable; and finalize and approve a plan for retiring the FDIC's legacy PIV card system.

Corporate Policies and Procedures Need To Be Established

By December 2016, the FDIC had issued PIV cards to the vast majority of eligible employees and contractor personnel and begun requiring the use of PIV cards for logical access to the Corporate network. However, we found that the FDIC did not have policies and procedures to govern these critical program activities. Specifically, the FDIC had not:

- issued a policy directive that defines key roles, responsibilities, and processes for managing PIV cards;

- established procedures for managing the issuance, termination, renewal, reissuance, and destruction of PIV cards;

- established policies and procedures governing the use of PIV cards for logical access; or

- updated its existing telework and security policies to address the use of PIV cards.

In the absence of formal policies and procedures, the FDIC's ACP Steering Committee, which had oversight responsibility for the ACP, made decisions to address process issues as they arose. Typically, these decisions were conveyed to FDIC employees and contractor personnel through e-mails. For example, the Committee made decisions pertaining to the types of:

- users and network devices exempt from using PIV cards and the associated processes for requesting and granting exceptions, and

- FDIC users required to use USB tokens as a temporary back-up when they forget or lose their PIV card.

Although email offers a means of quickly disseminating information, it is not a substitute for formal policies and procedures. Absent formal policies and procedures, employees and contractor personnel may not become aware of, or fully understand and properly carry out, management's expectations. In addition, employees and contractor personnel may not implement processes in a repeatable, consistent, or disciplined manner. In our view, the FDIC did not establish policies and procedures because its priority was meeting an aggressive timeline for issuing PIV cards and implementing MFA.

Further, the CIO Organization planned to deploy PIV-enabled laptop computers to any employee or contractor personnel who did not already have an FDIC-issued laptop to ensure (among other things) they can telework when needed, such as during an emergency. CIO Organization staff informed us that after they complete the laptop deployment, only FDIC-furnished computers will be permitted to access the Corporate network. We noted that existing telework and security policies do not address the use of PIV cards to access the Corporate network and allow employees to use their personal computers to remotely access the network. The FDIC should ensure that processes are in place to support this change in business practice and that the change is communicated to employees and contractor personnel in a timely manner. Doing so will result in more successful and effective telework arrangements and greater assurance that telework can support continuity of operations in the event of an emergency.

Recommendations

We recommend that the Director, DOA:

1. Issue a Corporate policy directive and associated procedures to govern the issuance and maintenance of PIV cards.

We recommend that the FDIC's CIO, in coordination with DIT and DOA:

2. Establish policies and procedures to govern the use of PIV cards to support logical access to the Corporate network.

Reliable Data Needed For Contractor PIV Card Management

The FDIC maintains a number of information systems that contain personnel data about contractors. Such systems include the Corporate Human Resources Information System-Human Resources (CHRIS-HR), legacy PIV card system, Physical Access Control System, and internal email system.[13] Of these systems, CHRIS-HR plays a particularly important role in the issuance and maintenance of PIV cards because the FDIC uses it to provide personnel data to the USAccess program.

Based on our review of relevant documentation and discussions with DOA and DIT staff, we learned that none of the systems referenced above contain all of the data needed to support issuing and maintaining PIV cards for FDIC contractor personnel. In addition, contractor data in these systems were not always current, accurate, or complete. For example, the systems frequently did not reflect the departure of contractor personnel or identify whether contractor personnel had a completed background check. To obtain reliable contractor information, DOA and DIT staff reconciled data among various information systems and verified the data with information provided by the FDIC's contract oversight managers and records maintained by the U.S. Office of Personnel Management.

Because CHRIS-HR was not a reliable source of contractor personnel information, the FDIC could not efficiently identify those contractor personnel who needed a PIV card or gather reliable information needed to issue those personnel PIV cards. This, in turn, negatively affected the accuracy of internal FDIC reports describing the Corporation's progress towards its goal of issuing PIV cards to 90 percent of eligible employees and contractor personnel by September 30, 2016.[14]

The use of reliable information to support business decision-making is a basic tenet of an effective internal control system. Absent reliable contractor personnel data, PIV cards may not be issued or revoked in a timely manner, presenting an increased risk of unauthorized access to FDIC facilities and the Corporate network.

[13] CHRIS-HR is the FDIC's authoritative system of record for managing personnel information. The Physical Access Control System is used to manage employee and contractor access at FDIC-controlled facilities.

[14] The FDIC reported its progress as the percentage of PIV cards issued to eligible employees and contractor personnel (i.e., the ratio of PIV cards issued to the total population of eligible employees and contractor personnel). Because the population of contractor personnel requiring PIV cards was not reliable, the FDIC's progress reporting was not fully accurate.

Recommendation

We recommend that the Director, DOA:

3. Take steps to ensure the reliability of contractor personnel data in CHRIS-HR.

A Plan for Retiring the FDIC's Legacy PIV Card System Is Needed

The FDIC's legacy PIV card system experienced frequent hardware and software failures. For example, the system's cameras and printers used in generating PIV cards frequently malfunctioned, and the system was often unavailable for extended periods of time. Thus, it was difficult for DOA to produce PIV cards for employees and contractor personnel. These same shortcomings also limited the FDIC's ability to provide support services to existing PIV cardholders, such as resetting PINs and troubleshooting PIV cards that would not allow users to access to the Corporate network. Further, the USAccess program could not assist the FDIC in addressing these issues because the system used by the USAccess program is not compatible with the FDIC's legacy PIV card system. As a result, the FDIC placed priority attention on replacing existing PIV cards issued by the legacy PIV card system with new PIV cards issued through the USAccess program.

The ACP Steering Committee began considering options for retiring the FDIC's legacy PIV card system as early as October 2016. However, the Committee had not made a decision regarding the timing and approach for retiring the system by the close of our audit field work in December 2016. The FDIC needed to develop a written plan for retiring the FDIC's legacy PIV card system that reflects consideration of relevant costs, risks, and potential business needs. Doing so would be a prudent business practice.

With respect to costs, a presentation to the ACP Steering Committee in October 2016 indicated that the FDIC's legacy PIV card system would cost about $390,000 to maintain through September 2017. The FDIC projected that, by then, all PIV cards issued by the legacy system would have been replaced by PIV cards issued through the USAccess program. Given the large number of PIV cards issued by the legacy system that still remain active, there may be a need to maintain the legacy system for a period of time to provide technical support services.[15] In addition, because the system contains personally identifiable information, such as names, addresses, and fingerprint images, the plan for retiring the system should include steps to ensure the timely and safe disposal of this information.

[15] According to the FDIC's *PIV Inventory Executive Dashboard*, approximately 3,100 PIV cards issued by the FDIC's legacy PIV card system were active as of November 29, 2016.

Recommendation

We recommend that the FDIC's CIO, in coordination with DIT and DOA:

4. Develop and approve a plan for retiring the FDIC's legacy PIV card system.

Status of Credentialing and Multifactor Authentication

According to information in the FDIC's *PIV Inventory Executive Dashboard*, as of December 19, 2016, the FDIC had issued PIV cards to 7,645 of 8,166 (or 94 percent) eligible employees and contractor personnel. A DIT representative reported that the majority of individuals who had not been issued PIV cards as of that date were contractor personnel. In addition, as of the same date, the *PIV Inventory Executive Dashboard* indicated that 492 (or 98 percent) of the FDIC's privileged users had been issued a PIV card. As discussed earlier, the U.S. CIO has indicated that implementing MFA for privileged users is an especially important step that federal agencies can take to protect their networks, systems, and data from unauthorized access.

With respect to MFA, the FDIC began requiring all eligible employees and contractor personnel to use their PIV card to authenticate to the Corporate network via desktop and laptop computers effective December 29, 2016.

Corporation Comments and OIG Evaluation

The CIO and Directors, DOA and DIT, provided a joint written response, dated June 6, 2017, to a draft of this report. The response is provided in its entirety in Appendix 3. In the response, FDIC management concurred with all four of the report's recommendations. In addition, subsequent to the issuance of our draft report, FDIC management provided us with an approved plan for the retirement of the FDIC's legacy PIV card system. We determined that the plan is responsive to Recommendation 4 and have closed the recommendation. Management's planned corrective actions for the remaining three recommendations are responsive and resolved, but will remain open until we confirm that corrective actions have been completed. A summary of the Corporation's corrective actions is presented in Appendix 4.

Objective, Scope, and Methodology

Objective

The audit objective was to assess the FDIC's plans and actions to address the recommendations contained in the ICAM Audit Report. We conducted this performance audit from January 2016 through December 2016 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Scope and Methodology

To address the objective, we gained an understanding of relevant concepts and requirements related to credentialing and MFA, as well as the FDIC's activities in these areas, by reviewing (among other things):

- HSPD-12
- NIST FIPS PUB 199, 201, and 201-2
- NIST Cybersecurity White Paper, entitled *Best Practices for Privileged User PIV Authentication*, dated April 21, 2016
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013
- NIST SP 800-63-2, *Electronic Authentication Guideline*, dated August 2013
- OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 5, 2005
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, dated October 30, 2015
- Literature pertaining to GSA's USAccess program
- Audit reports issued by the Government Accountability Office (GAO) and FDIC OIG, most notably GAO's report, entitled *PERSONAL ID VERIFICATION: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, dated September 2011, and the ICAM Audit Report issued in September 2015
- Relevant FDIC policies, procedures, and guidance, such as Circular 2121.1, *FDIC Telework Program*, dated December 21, 2012

Objective, Scope, and Methodology

To determine whether the actions taken by FDIC management to address the recommendations were responsive and supported the closure of the recommendations, we:

- reviewed the FDIC's corrective action closure forms and other relevant documentation, such as the ACP business case, project charter, communications plan, project plans, budget, and expense data;

- evaluated project management documentation and analyses prepared by DIT and DOA, including ACP Executive Steering Committee and ACP Steering Committee meeting minutes and briefings;

- spoke with representatives of DOA, DIT, the CIO Organization, and the Division of Finance's Corporate Management Control who had responsibility for implementing, managing, and/or reporting on corrective actions; and

- attended meetings of the ACP Executive Steering Committee, ACP Steering Committee, and ACP Working Group where project goals, risks, budgets, and status were discussed.

The scope of the audit was limited to reviewing activities involving credentialing and MFA involving PIV cards. We did not assess activities associated with other components of the ACP program. In addition, the scope of our work related to logical access was limited to using the PIV card to access the Corporate network via desktop and laptop computers. The audit did not address logical access involving mobile computing devices other than laptops (such as iPADs, iPhones, or BlackBerrys) or outsourced provider systems or services. We briefed the Directors, DOA and DIT, and the FDIC Audit Committee in April 2016 on the status of the FDIC's efforts to address the recommendations in the ICAM Audit Report, as well as progress relative to goals and expectations and efforts to mitigate significant risks. In January 2017, we briefed DOA, DIT, and CIO Organization officials on our preliminary audit results and recommendations. Except as described in the report, our results are as of December 2016.

We did not perform audit procedures to assess controls over the reliability of data in FDIC information systems because such procedures were not necessary to accomplish our audit objective. We did, however, rely on certain data in the *PIV Inventory Executive Dashboard* to determine the status of the FDIC's credentialing and MFA activities. We determined that data in the dashboard pertaining to the percentage of employees and contractor personnel who had been issued PIV cards were not fully reliable because the data were based, in part, on contractor personnel data contained in the CHRIS-HR system that were not reliable. In this regard, our report includes a recommendation designed to improve the reliability of contractor personnel data in CHRIS-HR.

Objective, Scope, and Methodology

Where automated data in the *PIV Inventory Executive Dashboard* were significant to our audit results, we performed audit procedures to gain a general understanding of how the data were developed and we corroborated the data to the extent possible through basic reasonableness checks against other sources to identify obvious inconsistency or completeness errors. In this manner, we were able to determine that, notwithstanding the limitations of the contractor personnel data in CHRIS-HR, the information was sufficiently reliable for the purposes of our report.

Although we considered the policy statements and recommended practices in HSPD-12, OMB memoranda, and NIST publications referenced in this report, we did not assess the FDIC's compliance with laws and regulations because doing so was not necessary to accomplish our audit objective. We assessed the risk of fraud and abuse related to our audit objective 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

Acronym/Abbreviation	Explanation
ACP	Access Control Program
CHRIS-HR	Corporate Human Resource Information System-Human Resources
CIO	Chief Information Officer
DIT	Division of Information Technology
DOA	Division of Administration
FDIC	Federal Deposit Insurance Corporation
FIPS PUB	Federal Information Processing Standards Publication
GAO	Government Accountability Office
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
ICAM	Identity Credential and Access Management
IT	Information Technology
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
SP	Special Publication
USB	Universal Serial Bus

Corporation Comments

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226
Division of Administration

DATE: June 6, 2017

MEMORANDUM TO: Mark Mulholland, Assistant Inspector General for Information Technology Audits and Cyber

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

Lawrence Gross, Jr. **/Signed/**
Chief Information Officer

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

SUBJECT: Management Response to the OIG Draft Report Entitled, Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program (Assignment No. 2016-022)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft audit report entitled Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program (Assignment No. 2016-022), dated April 24, 2017.

We appreciate the OIG's analysis and findings regarding the FDIC's credentialing and multifactor authentication efforts. We particularly appreciate the OIG's determination that the corrective actions taken by the FDIC to address the original ICAM Audit Report recommendations adequately resolved the audit report's concerns and recommendations. We recognize the need to further address remaining risks and have made, and continue to make, changes to the ICAM Program to reflect that need.

The audit report identifies four recommendations for improvements to strengthen information security. FDIC management concurs with the report's findings and is committed to addressing each of the OIG's recommendations to further strengthen the security of FDIC's facilities and corporate network. Our response below contains actions already completed, planned or in process.

Recommendation 1: The OIG recommends that the Director, Division of Administration (DOA) issues a Corporate policy directive and associated procedures to govern the issuance and maintenance of PIV cards.

Management Decision: Concur

Corporation Comments

Corrective Actions:

DOA Response: DOA is establishing a new PIV card issuance and maintenance directive. The directive entitled "Personal Identity Verification (PIV) Card Program" establishes the FDIC PIV Card Program and the requirement to use the PIV card as the sole authorized identification card to gain physical access to FDIC owned/leased space and logical access to FDIC information systems.

In February 2017, the Access Control Program Steering Committee reviewed and approved the draft directive. The directive is now being vetted through other stakeholders including DOA's Labor and Employee Relations and the Legal Division. Their approval is expected shortly.

Additionally, DOA updated the PIV Card Issuer (PCI) Operations Plan and its Standard Operating Procedures. These comprehensive documents describe all functions and responsibilities required to produce, issue and maintain PIV credentials for the FDIC in support of its implementation of the USAccess managed service program.

Estimated Completion Date: July 31, 2017

Recommendation 2: The OIG recommends that the Chief Information Officer (CIO), in coordination with the Director, Division of Information Technology (DIT), and Director, Division of Administration (DOA) establish policies and procedures to govern the use of PIV cards to support logical access to the Corporate network.

Management Decision: Concur

Corrective Actions:

CIO Response: The CIO Organization revised its procedures to address the roles, responsibilities, expectations and governance of logical access to the corporate network via PIV cards. DIT has developed a comprehensive set of Help Desk work instructions and Standard Operating Procedures (SOPs) to manage PIV-related inquiries and issues. In addition, DIT Client Support Services has established and implemented new workflow for issuing all new employees and contractors a Safenet token during the onboarding process. The token allows for and enforces MFA to the FDIC network while the new employee or contractor is in the process of getting their PIV card. These actions were completed by January 27, 2017. Additionally, the CIO Organization, in a combined policy document with DOA, will define authorities, roles and responsibilities for PIV logical access.

DOA Response: DOA is in the process of issuing a new Directive entitled: Personal Identity Verification (PIV) Card Program (see DOA response under recommendation #1). This Directive will formally establish the PIV Card Program and the requirement to use the PIV Card for physical and logical access. DOA expects to issue the new Directive by July 31, 2017.

Corporation Comments

In addition, the FDIC's current telework program directive addresses policy and guidelines for accessing FDIC systems along with safeguarding FDIC information while teleworking. As necessary, DOA will update its telework program directive to reflect any future policy changes that might impact how employees are allowed to access FDIC systems while teleworking.

Estimated Completion Date: July 31, 2017

Recommendation 3: The OIG recommends that the Director, Division of Administration (DOA) take steps to ensure the reliability of contractor personnel data in CHRIS-HR.

Management Decision: Concur

Corrective Actions:

DOA Response: DOA will take a two-phased approach to ensure the reliability of contractor personnel data in CHRIS HR. First, DOA will establish a multi-divisional working group to create a formal plan for updating and maintaining contractor data in CHRIS HR or other appropriate system. The plan will designate DOA as the process owner, identify roles and responsibilities of key stakeholders, develop timeframes for implementation of new procedures, as well as develop controls for periodically validating the accuracy and completeness of contractor data, and establish guidelines for developing policies and procedures as appropriate. The working group will be comprised of DOA and DIT officials and others as necessary. The initial deliverable from this group will be a planning document to be completed by July 31, 2017.

Second, DOA will fully implement the working group's plan to ensure that the CHRIS HR system contains current, accurate, and complete contractor personnel data. This will be completed by December 31, 2017.

Estimated Completion Dates: Planning document by July 31, 2017. Full implementation by December 31, 2017.

Recommendation 4: The OIG recommends that the Chief Information Officer (CIO), in coordination with the Director, Division of Information Technology (DIT), and Director, Division of Administration (DOA) develop and approve a plan for retiring the FDIC's legacy PIV card system.

Management Decision: Concur

Corrective Actions:

CIO Response: The CIO will decommission the web servers, application servers, and databases by September of this year.

Corporation Comments

Estimated Completion Date: September 1, 2017

Actions Completed to Date: DIT and DOA initiated a plan to migrate all legacy cardholders to PIV cards issued by GSA USAccess by the end of June this year. This plan was approved by the Access Control Program Steering Committee on February 5, 2017. The plan provides specific timelines for the collection, removal, and destruction of legacy cards and the return of badging equipment.

Date Actions Were Completed: February 5, 2017

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 Closed[b]
1	DOA will establish a policy directive addressing PIV card issuance and maintenance. DOA has already updated its PIV Card Issuer Operations Plan and standard operating procedures to describe the functions and responsibilities required to produce, issue, and maintain PIV cards.	7/31/2017	No	Yes	Open
2	The CIO Organization will establish a policy directive addressing authorities, roles, and responsibilities pertaining to the use of PIV cards for logical access. The CIO Organization has already revised its procedures to address roles, responsibilities, expectations, and governance for logical access to the Corporate network via the PIV card. In addition, DIT has developed Help Desk instructions and standard operating procedures to manage PIV-related inquiries and issues as well as workflows for issuing Safenet tokens to new employees and contractor personnel during the onboarding process.	7/31/2017	No	Yes	Open
3	DOA, working in coordination with DIT, will develop a formal plan for updating and maintaining contractor data in CHRIS HR (or other appropriate system). The plan is expected to be completed by July 31, 2017. DOA will fully implement the plan by December 31, 2017.	12/31/2017	No	Yes	Open

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
4	The Access Control Program Steering Committee approved a plan for the retirement of the FDIC's legacy PIV card system.	2/5/2017	No	Yes	Closed

[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 the OIG confirms that corrective actions have been completed and are responsive.