The FDIC's Privacy Program

December 2019 **AUD-20-003**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

REDACTED VERSION

PUBLICLY AVAILABLE

Portions of this report containing sensitive information have been redacted and are marked accordingly.

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Executive Summary

The FDIC's Privacy Program

In fulfilling its legislative mandate, the Federal Deposit Insurance Corporation (FDIC) collects and maintains significant quantities of Personally Identifiable Information (PII) on bankers and financial institution customers. In addition, as a Federal employer and acquirer of services, the FDIC collects significant amounts of PII on its employees and contractors. Such PII includes, for example, names, home addresses, Social Security Numbers, dates and places of birth, personal financial information, employment histories, education and healthcare information, and the results of background investigations.

As of June 2018, the FDIC reported that it maintained 338 information systems containing PII, and 174 of these systems contained sensitive PII, as defined by the FDIC. However, this did not include data containing PII stored on the FDIC's internal network shared drives or in hard copy format. The significant amount of PII held by the FDIC underscores the importance of implementing an effective Privacy Program that ensures proper handling of this information and compliance with privacy laws, policies, and guidelines.

Congress has enacted a number of statutes that impose privacy-related requirements on Federal agencies. In addition, the Office of Management and Budget (OMB) has issued Government-wide policies and guidance to assist agencies in fulfilling their statutory responsibilities related to privacy. In July 2016, OMB issued a revised version of its Circular A-130, *Managing Information as a Strategic Resource* (OMB Circular A-130), which updated and expanded agency requirements and responsibilities for managing PII. Appendix II of OMB Circular A-130 organized relevant privacy-related requirements and responsibilities for Federal agencies into nine areas.

The objective of the audit was to assess the effectiveness of the FDIC's Privacy Program and practices. We assessed effectiveness by performing audit procedures to determine whether the FDIC's privacy controls and practices complied with selected requirements defined in eight of the nine areas covered by Appendix II of OMB Circular A-130.

Results

We found that the Privacy Program controls and practices we assessed were effective in four of eight areas examined. Notably, the FDIC implemented a privacy awareness and training program; identified its privacy staffing and budgetary needs; established privacy competency requirements for key staff; and took steps to ensure contractor compliance with privacy requirements.

However, the FDIC's controls and practices for its Privacy Program in the other four areas assessed were either partially effective or not effective, because they did not comply with all relevant privacy laws and/or OMB policy and guidance. Specifically, the FDIC did not:

- Fully integrate privacy considerations into its risk management framework designed to categorize information systems, establish system privacy plans, and select and continuously monitor system privacy controls;
- Adequately define the responsibilities of the Deputy Chief Privacy Officer or implement Records and Information Management Unit (RIMU) responsibilities for supporting the Privacy Program;
- Effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII within established timeframes; and
- Ensure that Privacy Impact Assessments were always completed, monitored, and retired in a timely manner.

Weaknesses in the FDIC's Privacy Program increased the risk of PII loss, theft, and unauthorized access or disclosure, which could lead to identity theft or other forms of consumer fraud against individuals. For example, in response to concerns raised during our audit, the Chief Information Security Officer scanned all network shared drives and identified 986 instances in which access to sensitive information may not be properly restricted. In addition, weaknesses related to the management of Privacy Impact Assessments reduced transparency regarding the FDIC's practices for handling and protecting PII.

Recommendations

Our report contains 14 recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and records management practices. We recommended that the FDIC update its policies and procedures and establish appropriate governance to ensure proper execution of privacy responsibilities. We also recommended that the FDIC implement privacy plans for all information systems containing PII consistent with OMB policy; continuously monitor privacy controls;

effectively manage and protect PII stored in network shared drives and in hard copy; implement records management requirements; and revise processes to improve the management of Privacy Impact Assessments. These recommendations will help ensure that the FDIC properly secures and manages its PII holdings in accordance with Federal requirements and effectively manages privacy-related risks. The FDIC concurred with all 14 recommendations and plans to complete corrective actions by December 17, 2021.

Contents

Background **3**

OMB Policies and Guidance 4
The FDIC's Privacy Program Organizational Structure 7
Managing Information Security and Privacy Risks 9

Audit Results **12**

Privacy Not Fully Integrated into the FDIC's Risk Management Framework 14
Privacy-Related Roles and Responsibilities Not Adequately Defined or Implemented 20
PII Not Effectively Managed 24
Minimization of PII Records Not Effectively Implemented 27
Effectiveness of PIA Process Needed Improvement 31

FDIC Comments and OIG Evaluation **33**

Appendices

1. Objective, Scope, and Methodology 34
2. Summary of Audit Results 37
3. Acronyms and Abbreviations 40
4. Relationship Between Security and Privacy 41
5. Minimization Issues 42
6. OIG Memorandum Regarding Unsecured Sensitive Information on Network Shared Drives 44
7. Management's Response to OIG Memorandum Regarding Unsecured Sensitive Information on Network Shared Drives 46
8. FDIC Comments 49
9. Summary of the FDIC's Corrective Actions 57

Figures

1. Key Privacy-Related Roles 8
2. Organization-Wide Risk Management 10
3. The Risk Management Framework 11
4. Effectiveness of Privacy Controls and Practices by Control Area 13
5. Chronology of Risk Management Framework Guidance and Implementation 17
6. Relationship Between Security and Privacy 41

Tables

1. Privacy Requirements and Responsibilities in OMB Circular A-130, Appendix II 5
2. OIG Assessment of Selected Privacy Requirements in OMB Circular A-130 37

December 18, 2019

Subject | ***The FDIC's Privacy Program***

In fulfilling its legislative mandate, the Federal Deposit Insurance Corporation (FDIC) collects and maintains significant quantities of Personally Identifiable Information (PII)[1] on bankers and financial institution customers. In addition, as an employer and acquirer of services, the FDIC maintains significant amounts of PII related to its employees and contractors. PII maintained by the FDIC includes, but is not limited to, names, home addresses, Social Security Numbers (SSN), dates and places of birth, personal financial information, employment histories, education and healthcare information, and the results of background investigations.

As of June 2018, the FDIC reported that it maintained 338 information systems containing PII. The FDIC reported that 174 of these information systems contained sensitive PII.[2] However, these information systems did not include PII stored on the FDIC's internal network shared drives[3] or in hard copy format. The significant amount of PII held by the FDIC underscores the importance of implementing an effective Privacy Program that ensures proper handling of this information and compliance with privacy laws, policies, and guidelines.

An effective Privacy Program provides assurance that the FDIC is properly safeguarding the personal information within its custody and implementing controls to mitigate potential breaches.[4] Breaches can expose individuals to identity theft or other types of consumer fraud, which can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and in rare cases, risk to personal safety. Breaches can also result in unnecessary costs, potential legal liability, and reputational harm for the FDIC.

[1] The Office of Management and Budget's (OMB) Circular A-130, *Managing Information as a Strategic Resource* (OMB Circular A-130) (July 2016) defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."
[2] According to FDIC Circular 1360.9, *Protecting Sensitive Information*, (October 2015), sensitive PII is a subset of PII that presents the highest risk of being misused for identity theft or fraud. Sensitive PII may be comprised of a single item of information, such as a SSN, or a combination of two or more items, such as full name along with financial, medical, criminal, or employment information.
[3] Network shared drives make information accessible to multiple users or groups of users over a network.
[4] According to OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 2017), a breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) an individual other than the authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose."

During 2016, the FDIC reported a series of breaches to Congress as departing employees improperly downloaded sensitive PII, including SSNs, to removable media devices shortly before leaving the FDIC. Collectively, these breaches potentially affected over 121,000 individuals. We reported on the FDIC's handling of these breaches and its associated controls in four prior reports.[5] Collectively, these four reports contained 36 recommendations intended to strengthen the FDIC's security and privacy controls, particularly relating to the FDIC's breach response practices and reporting and associated notifications to Congress. We closed all but one of these prior recommendations. We recently issued four other reports wherein we recommended improvements to address weaknesses in the FDIC's information security management practices.[6]

The objective of this audit was to assess the effectiveness of the FDIC's Privacy Program and practices. We assessed effectiveness by performing audit procedures to determine whether the FDIC's privacy controls and practices complied with selected provisions in privacy-related statutes, OMB policy and guidance, and FDIC policies and procedures.[7] We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report provides additional details about our objective, scope, and methodology; Appendix 2 contains our analysis of the FDIC's compliance with privacy-related requirements in Appendix II of OMB Circular A-130; Appendix 3 contains a list of acronyms and abbreviations; Appendix 4 describes the relationship between security and privacy; Appendix 5 describes instances in which the FDIC did not dispose of PII in a timely manner; Appendix 6 contains a memorandum issued by the OIG to the FDIC's Chief Information Officer (CIO)/Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) regarding the urgent need to properly secure PII on network shared drives; Appendix 7 contains management's response to the OIG memorandum; and Appendix 8 and Appendix 9 contain the FDIC's comments on this report and a summary of the FDIC's corrective actions.

[5] *See* Office of Inspector General (OIG) Reports, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (FDIC OIG AUD-16-004) (July 2016, revised February 2017); *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (FDIC OIG AUD-17-006) (September 2017); *Controls over Separating Personnel's Access to Sensitive Information* (FDIC OIG EVAL-17-007) (September 2017); and *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (FDIC OIG-18-001) (April 2018).
[6] *See* OIG Reports, *The FDIC's Governance of Information Technology Initiatives* (FDIC OIG AUD-18-004) (July 2018); *Controls Over System Interconnections with Outside Organizations* (FDIC OIG AUD-19-002) (December 2018); *Preventing and Detecting Cyber Threats* (FDIC OIG AUD-19-005) (May 2019); and *The FDIC's Information Security Program – 2019* (FDIC OIG AUD-20-001) (October 2019).
[7] *See* Appendix 2 for a description of the privacy controls and practices we assessed.

BACKGROUND

Congress has enacted a number of statutes that impose privacy-related requirements on Federal agencies. Such statutes include the Privacy Act of 1974[8] (the Privacy Act), Section 208 of the E-Government Act of 2002[9] (the E-Gov Act), Section 522 of the Consolidated Appropriations Act of 2005[10] (2005 Consolidated Appropriations Act), and the Federal Information Security Modernization Act of 2014 (FISMA).[11]

The Privacy Act requires Federal agencies to establish rules and procedures for maintaining and protecting personal data in agency systems of record.[12] This statute permits individuals to access records pertaining to them that Federal agencies collect, maintain, use, and disseminate. The statute also prohibits the disclosure of an individual's records without his or her consent, unless the disclosure is permitted by another provision in the Act. Further, the Privacy Act requires agencies to ensure that any records containing information about an individual are for necessary and relevant purposes, that the records are current and accurate for their intended use, and that agencies provide adequate safeguards to prevent misuse of such information.

The E-Gov Act requires Federal agencies to conduct Privacy Impact Assessments (PIA) of information technology (IT) and collections of information and make the PIAs available to the public. A PIA is a process for examining the risks of using IT to collect, maintain, and disseminate PII from or about members of the public. When an agency conducts PIAs, it can identify and evaluate protections and processes to mitigate the privacy impacts of collecting such information.

The 2005 Consolidated Appropriations Act requires Federal agencies to designate a CPO with primary responsibility for agency privacy and data protection policies. According to this statute, the CPO is responsible for assuring:

- The use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of PII.

[8] Privacy Act of 1974, 5 U.S.C. § 552a.
[9] Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. § 3501 note).
[10] Section 522 of the Consolidated Appropriations Act of 2005, Pub. L. No. 108-447, 118 Stat. 2809, amended by Consolidated Appropriations Act of 2008, Pub. L. No. 110-161, 121 Stat. 1844 (codified as amended at 42 U.S.C. § 2000ee-2).
[11] Pub. L. No. 113-283 (December 2014).
[12] According to the Privacy Act, a system of record is a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information particularly assigned to the individual.

- Technologies used to collect, use, store, and disclose PII allow for continuous auditing of compliance with stated privacy policies and practices.
- Compliance with fair information practices as defined in the Privacy Act of 1974 for personal information contained in systems of record.
- Adequate training and education for employees on privacy and data protection policies to promote awareness of, and compliance with, established privacy and data protection policies.
- The agency protects PII and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Compliance with the agency's established privacy and data protection policies.

FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information (including PII) and information systems. This includes information systems provided or managed by another agency, contractor, or other source.

OMB Policies and Guidance

OMB has issued various Government-wide policies and guidance to assist Federal agencies in fulfilling their statutory responsibilities related to privacy. These policies and guidance reinforce the importance of establishing comprehensive privacy programs and designating an individual with primary responsibility to oversee the agency's privacy program and ensure compliance with applicable privacy requirements.

On February 11, 2005, OMB issued Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy* (OMB Memorandum M-05-08), which directed Federal agency heads to designate a Senior Agency Official for Privacy (SAOP) to have overall agency-wide responsibility for information privacy issues. According to OMB Memorandum M-05-08, the SAOP has responsibility and accountability for ensuring the agency's implementation of information privacy protections and compliance with Federal laws, such as the Privacy Act, regulations, and policies relating to information privacy. OMB Memorandum M-05-08 states that the agency CIO may perform this role. On March 9, 2005, the FDIC Chairman designated the CIO to serve as the CPO. At the FDIC, the CPO has the same responsibilities as the SAOP.

On July 28, 2016, OMB revised OMB Circular A-130 to address changes in the law and advances in technology.[13] OMB also revised the circular to ensure consistency with Executive Orders, Presidential Directives, OMB policy, and standards and guidelines issued by the National Institute of Standards and Technology (NIST).[14] OMB Circular A-130, Appendix II, *Responsibilities for Managing PII,* organizes privacy-related requirements and responsibilities into nine control areas. As described in Appendix 1 of this report, OMB Circular A-130, Appendix II, was the principal criteria against which we assessed the FDIC's Privacy Program and practices. We assessed the effectiveness of the FDIC's privacy controls and practices in all but one of the nine control areas in Table 1. We did not assess the *Incident Response* control area because the OIG evaluated this control area in previous audits.

Table 1: Privacy Requirements and Responsibilities in OMB Circular A-130, Appendix II

Privacy Control Area	Description
1. General Requirements	Establish and maintain a privacy program, comply with privacy requirements, and manage privacy risks. Activities in this area include developing privacy program plans; designating an SAOP; and monitoring Federal privacy-related laws, regulations, and policies for changes.
2. Considerations for Managing PII	Maintain an inventory of PII; regularly review all PII held by the agency; eliminate the unnecessary collection, maintenance, and use of PII; and follow approved records retention or disposition schedules.
3. Budget and Acquisition	Ensure that agency privacy programs have the resources necessary to manage PII and consider privacy when acquiring or developing system technologies and services.
4. Contractors and Third Parties	Ensure that contractors and other third parties handling PII on behalf of the agency comply with privacy requirements. This includes incorporating privacy into agency contracts and other agreements.
5. Privacy Impact Assessments	Conduct PIAs in accordance with the E-Gov Act and OMB policy.
6. Workforce Management	Assess and address privacy hiring, training, and professional development needs.

[13] OMB issued the prior version of Circular No. A-130, entitled *Management of Federal Information Resources*, on November 28, 2000.

[14] NIST is a non-regulatory Federal agency within the U.S. Department of Commerce. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems. NIST documents and communicates required security standards within Federal Information Processing Standards (FIPS) publications and recommended guidelines within NIST Special Publications (SPs).

Privacy Control Area	Description
7. Training and Accountability	Provide an agency-wide privacy awareness and training program for all employees and contractors and hold personnel accountable for non-compliance with privacy requirements.
8. Incident Response	Develop and implement incident management and response capabilities, including policies, roles and responsibilities, reporting, and periodic testing of effectiveness.
9. Risk Management Framework	Use the Risk Management Framework developed by NIST to manage privacy risks.

Source: OIG analysis of OMB Circular A-130, Appendix II.

On September 15, 2016, OMB issued Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy,* (OMB Memorandum M-16-24), which required agencies to develop, implement, and maintain an agency-wide privacy program led by an SAOP. The SAOP is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission. OMB Memorandum M-16-24 established the following three primary responsibilities for the SAOP.

Policy-Making. The SAOP shall have a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals that have privacy implications. According to OMB, in this role, "the SAOP shall ensure that the agency considers and addresses the privacy implications of all agency regulations and policies, and shall lead the agency's evaluation of the privacy implications of legislative proposals, congressional testimony, and other materials pursuant to OMB Circular A-19."[15]

Compliance. The SAOP shall have a central role in overseeing, coordinating, and facilitating the agency's privacy compliance efforts. This includes ensuring agency compliance with applicable privacy requirements in law, regulation, and policy including the Privacy Act of 1974, E-Gov Act, 2005 Consolidated Appropriations Act, OMB Circular A-130, and OMB Memorandum M-16-24 discussed above.

Risk Management. The SAOP shall manage privacy risks associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems.

[15] OMB Circular A-19, *Legislative Coordination and Clearance*, (Revised September 1979).

In addition, OMB Memorandum M-16-24 stated that:

> Agencies should recognize that privacy and security are independent and separate disciplines. While privacy and security require coordination, they often raise distinct concerns and require different expertise and different approaches. The distinction between privacy and security is one of the reasons that the Executive Branch has established a Federal Privacy Council independent from the Chief Information Officers Council.

Appendix 4 of this report provides information about the relationship, as well as the distinctions, between security and privacy.[16]

OMB Memorandum M-16-24 also required agencies to reassess their SAOP designations in light of advances in technologies that led to new challenges in protecting PII.[17] Pursuant to OMB Memorandum M-16-24, the FDIC completed an assessment of its Privacy Program on November 9, 2016 and concluded that its Privacy Program complied with existing law and OMB guidance and that the CIO should continue to serve as the SAOP.

The FDIC's Privacy Program Organizational Structure

In March 2013, the FDIC issued Directive 1360.20, *Privacy Program,*[18] formalizing the FDIC's Privacy Program. The directive articulates the FDIC's policy to protect the privacy of individuals and to collect, maintain, use, disseminate, and/or dispose of PII, in accordance with applicable Federal law and OMB guidance.
FDIC Directive 1360.20 assigns the CPO (designated as the FDIC's SAOP) overall agency-wide authority, responsibility, and accountability for information privacy issues and implementing information privacy protections. FDIC Directive 1360.20 also assigns the Information Security and Privacy Staff (ISPS)—which the FDIC reorganized into the Office of the Chief Information Security Officer (OCISO)—with responsibility for managing the FDIC's Privacy Program.

As previously noted, the FDIC reported a series of breaches to Congress during 2016. In 2017, the FDIC reorganized its privacy operations into a separate organizational unit within the OCISO called the Privacy Section. The FDIC implemented the reorganization to clarify separate responsibilities for privacy governance, incident response, and information security risk management. The

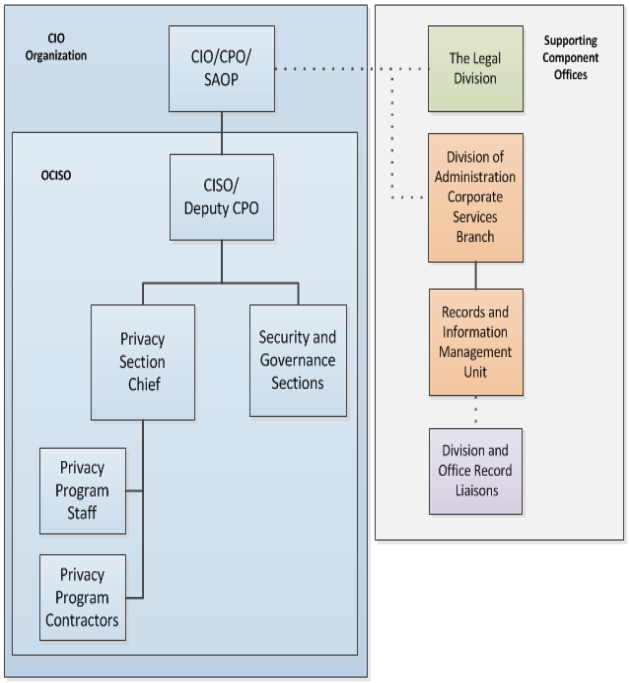
[16] As explained in Appendix 4, information security focuses on protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction. Privacy focuses on ensuring compliance with applicable privacy requirements and managing the risks associated with the collection, use, dissemination, storage, maintenance, disclosure, or disposal of PII.
[17] OMB Memorandum M-16-24 was issued in response to Executive Order 13719, *Establishment of the Federal Privacy Council*. On February 9, 2016, the President issued Executive Order 13719 to establish a permanent Federal Privacy Council. The Council serves as the principal interagency forum for improving how agencies address privacy throughout the Federal Government. Executive Order 13719 also directed OMB to issue a revised policy on the role and designation of the SAOP.
[18] FDIC Directive 1360.20 was updated in March 2017.

Privacy Section is led by a Section Chief and comprised of six Federal staff supported by six contractor staff.

Roles and Responsibilities

The FDIC issued its *Privacy Program Plan* in October 2017, and updated and reissued the plan in February 2019. The *Privacy Program Plan* provides an overview of the FDIC's Privacy Program and defines the structure, roles, and responsibilities for achieving the mission and vision of the Privacy Program.

Figure 1: Key Privacy-Related Roles



Source: FDIC Organizational Charts

FDIC Directive 1360.20 and the *Privacy Program Plan* designated positions within the CIO Organization and Divisions and Offices outside the CIO Organization with key privacy-related roles. These positions are illustrated in Figure 1 and described below.

SAOP. The SAOP is responsible for delivering an agency-wide risk-based Privacy Program to protect PII. In this role, the SAOP establishes and implements privacy and data protection policies and procedures pursuant to various statutory and regulatory requirements. As previously discussed, the SAOP also has a central policy-making role; ensures agency compliance with applicable privacy requirements in law, regulation, and policy; and manages privacy risk associated with the collection, storage, and disposal of PII.

CISO. The CISO serves as the Deputy CPO and principal advisor for the FDIC's Information Security and Privacy Programs. The CISO develops security and privacy policy, and establishes and manages the Privacy Program. The CISO reports directly to the SAOP.

Privacy Section Chief. The Privacy Section Chief advises the SAOP and Deputy CPO on the development, operation, and management of the Privacy Program. The Privacy Section Chief also manages the Privacy Program staff and contractors.

The Legal Division. The Legal Division assists the SAOP in ensuring compliance with the Privacy Act and the Paperwork Reduction Act.[19] For example, the Legal Division processes requests for information under the Freedom of Information Act[20] (FOIA) and manages System of Records Notices[21] for information systems and collections of records that contain PII.[22]

Records and Information Management Unit (RIMU) and Record Liaisons. RIMU and Record Liaisons oversee the lifecycle management (creation, management/use, and disposition) of business records and information (including PII) created or received by the FDIC. RIMU is a component office within the Division of Administration (DOA) Corporate Services Branch. The FDIC's Chief Operating Officer oversees DOA. RIMU and Record Liaisons provide advice and assistance to the Privacy Section to help ensure compliance with the FDIC Records Retention Schedule (RRS). The RRS classifies all FDIC business records, including records containing PII, and prescribes approved retention periods to ensure their timely destruction at the conclusion of the established retention period.

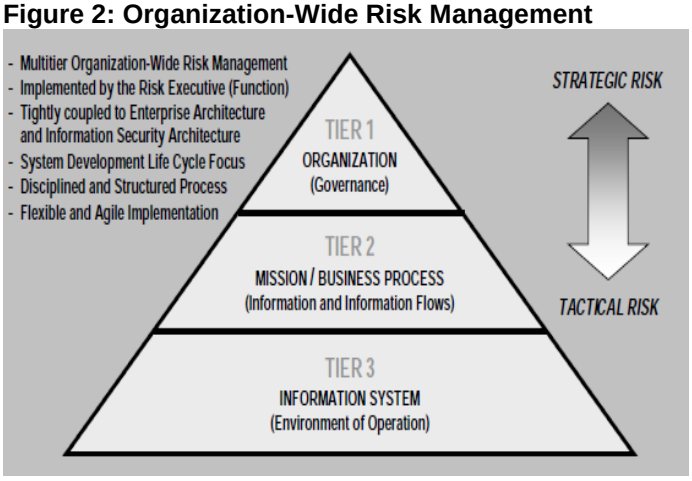
Managing Information Security and Privacy Risks

According to OMB Circular A-130, risk management is conducted as an agency-wide activity to ensure that risk-based decision-making is integrated into every aspect of the agency's planning and operations. NIST SP 800-37, Revision 1,[23] states that risk management is a holistic activity that is fully integrated into every aspect of an organization.

[19] Paperwork Reduction Act of 1995, 44 U.S.C. § 3501. The Paperwork Reduction Act states that prior to collecting any new information, agencies must publish notification in the Federal Register describing the proposed collection and an estimate of the burden resulting from the collection.
[20] Freedom of Information Act, 5 U.S.C. § 552.
[21] A System of Records Notice is an official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974. The System of Records Notice identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; and (iii) the categories of records maintained about individuals.
[22] On March 29, 2019, the FDIC Board of Directors delegated authority to the SAOP to authorize new and amended Privacy Act systems of records and their publication in the Federal Register.
[23] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010).

As reflected in Figure 2, NIST defines an approach to risk management that addresses risk-related concerns at three levels: *Level 1: Organization*, *Level 2: Mission/Business Process*, and *Level 3: Information System*.

Figure 2: Organization-Wide Risk Management



Source: NIST SP 800-37, Revision 1.

Risk management activities conducted at the *Organizational* and *Mission/Business Process* levels involve a wide range of functions, such as establishing a risk management strategy and organizational risk tolerance;[24] understanding threats to information systems and organizations; understanding the potential adverse effects on individuals; conducting organizational and system-level risk assessments; and identifying and prioritizing security and privacy requirements. Risk management activities conducted at the *Information System* level involve implementing the Risk Management Framework (RMF) defined in NIST SP 800-37, Revision 1 (described below).

At the FDIC, the Enterprise Risk Management (ERM) Program governs the risk management activities performed at the *Organizational* and *Mission/Business Process* levels. According to FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program*, the ERM Program operates as a joint-owned partnership between primary risk owners in the Divisions and Offices (such as the CIO Organization) and the Chief Risk Officer. The Chief Risk Officer leads the Risk Management and Internal Controls Branch within the Division of Finance. The ERM Program serves as the FDIC's risk executive function.[25]

Our audit did not evaluate the effectiveness of the FDIC's ERM Program or the risk management activities at the *Organization* and *Mission/Business Process* levels.[26]

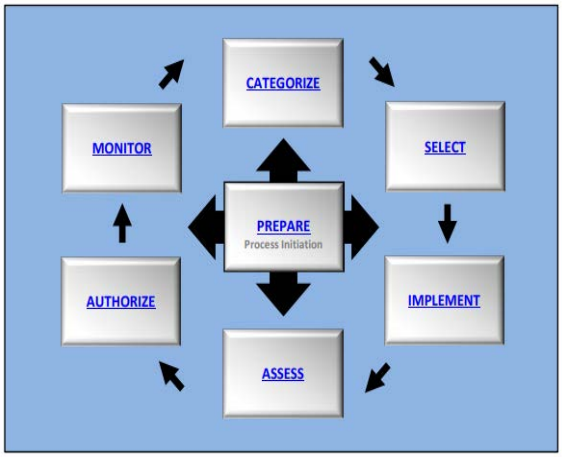
[24] According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), risk tolerance refers to the level of risk an entity is willing to assume in order to achieve a potential desired result.
[25] According to OMB Circular A-130, the risk executive function within an agency helps to ensure that managing information system-related risks is consistent across the agency, reflects the agency's risk tolerance, and is considered along with other agency risks affecting its missions or business functions.
[26] In April 2019, the OIG initiated a separate evaluation to assess the implementation and effectiveness of the FDIC's ERM program. As part of this separate evaluation, the OIG is reviewing the FDIC's ERM processes that facilitate the management and communication of information system-related security and privacy risk from a top-down and bottom-up approach.

Our audit focused on the FDIC's implementation of risk management activities at the *Information System* level, which includes the implementation of the RMF. According to OMB Circular A-130, effective implementation of the RMF ensures that managing information system-related risks aligns with the agency's mission or business objectives and overall risk management strategy, and risk tolerance established by the senior leadership through the risk executive function. OMB Circular A-130 further states that it is essential for agencies to take a coordinated approach in identifying and managing security and privacy risks. The scope of our audit included an assessment of the FDIC's integration of privacy into the RMF as prescribed by OMB Circular A-130.

Risk Management Framework

Traditionally, agencies used the RMF defined in NIST SP 800-37, Revision 1, to address security and related risks in the authorization process for information systems. OMB's Circular A-130 requires agencies to use the RMF to not only manage security risk, but privacy risk as well.[27] The RMF is one of the nine privacy control areas in Appendix II of OMB Circular A-130. To ensure consistency with OMB Circular A-130, in December 2018, NIST updated its RMF guidance and issued SP 800-37, Revision 2.[28] Revision 2 integrates security and privacy into the system development lifecycle to promote more informed, risk-based decisions. According to NIST SP 800-37, Revision 2, the RMF provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development lifecycle. As presented in Figure 3, implementing the updated

Figure 3: The Risk Management Framework



Source: NIST SP 800-37, Revision 2

[27] According to OMB Circular A-130 and NIST SP 800-37, it is important to understand the relationship—and particularly the distinctions—between information security and privacy. *See* Appendix 4 for a discussion about the relationship between information security and privacy.
[28] *See* NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018).

RMF consists of the following seven steps:

1. **Prepare** to execute the RMF from an organizational and information system level by establishing a context and priorities for managing security and privacy risks.

2. **Categorize** the information system and information processed, stored, and transmitted in the system based on four risk factors: impact of loss, threats, vulnerabilities, and likelihood of occurrence.[29]

3. **Select** controls for the information system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

4. **Implement** the controls and describe how to employ the controls within the information system and its environment of operation.

5. **Assess** the controls to determine whether they are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying security and privacy requirements.

6. **Authorize** the information system based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.

7. **Monitor** the information system and the associated controls on an ongoing basis to assess control effectiveness; document changes to the system and environment of operation; conduct risk assessments and impact analyses; and report the security and privacy posture of the system.

AUDIT RESULTS

We found that the Privacy Program controls and practices we assessed in four of eight control areas were effective.[30] Notably, the FDIC implemented a privacy awareness and training program; identified its privacy staffing and budgetary needs; established privacy competency requirements for key staff; and took steps to ensure that contractors complied with privacy requirements.

[29] NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012), encourages agencies to consider these risk factors during risk assessment activities.
[30] We assessed effectiveness by performing audit procedures to determine whether the FDIC's privacy controls and practices complied with selected provisions in privacy-related statutes and OMB policy and guidance. *See* Appendix 2 of this report for a detailed explanation of the controls we tested within eight of the nine key privacy areas of OMB Circular A-130.

However, the FDIC's controls and practices for its Privacy Program in the other four areas we assessed were either partially effective or not effective, because they did not comply with all relevant privacy laws, OMB policy and guidance, and FDIC policies and procedures. Specifically, the FDIC did not:

- Fully integrate privacy considerations into its risk management framework designed to categorize information systems, establish system privacy plans, and select and continuously monitor system privacy controls;
- Adequately define the responsibilities of the Deputy Chief Privacy Officer or implement RIMU responsibilities for supporting the Privacy Program;
- Effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII in accordance with its RRS; and
- Ensure that PIAs were always completed, monitored, and retired in a timely manner.

Figure 4 identifies the nine privacy control areas described in OMB Circular A-130, Appendix II, and our determinations regarding whether the FDIC's controls and practices in these areas were Effective, Partially Effective, or Not Effective.[31] We did not assess the effectiveness of controls or practices in the *Incident Response* control area, because our office had previously conducted audit work in this area.[32]

Figure 4: Effectiveness of Privacy Controls and Practices by Control Area

Privacy Control Area	Audit Result
1. General Requirements	▲
2. Considerations for Managing PII	▲
3. Budget and Acquisition	●
4. Contractors and Third Parties	●
5. Privacy Impact Assessments	▲
6. Workforce Management	●
7. Training and Accountability	●
8. Incident Response	-
9. Risk Management Framework	◆

●	Effective
▲	Partially Effective
◆	Not Effective
-	Not Assessed

Source: OIG analysis of selected privacy controls and practices described in OMB Circular A-130, Appendix II.

[31] Determinations of Effective indicate compliance with the privacy requirements and guidelines we assessed. Determinations of Partially Effective indicate compliance with some, but not all, of the privacy requirements and guidelines we assessed. Determinations of Not Effective indicate substantial non-compliance with the privacy requirements and guidelines we assessed.
[32] *See* OIG Reports, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (FDIC OIG AUD-16-004) (July 2016, revised February 2017), *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (FDIC OIG AUD-17-006) (September 2017); *Controls over Separating Personnel's Access to Sensitive Information* (FDIC OIG EVAL-17-007) (September 2017); and *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (FDIC OIG-18-001) (April 2018).

With respect to the *Considerations for Managing PII* control area, we identified unsecured sensitive PII stored on the FDIC's internal network shared drives. In addition, as part of a separate audit conducted by our office,[33] we discovered unsecured sensitive PII stored in FDIC facilities in hard copy format. The unsecured PII we found included, but was not limited to, FDIC employee and bank customer credit information, tax returns, and reports containing the names, SSNs, and dates of birth of individuals. We notified the CIO, CISO, and other management officials of the vulnerable PII during this audit, and they indicated that they would be taking further corrective actions. The lack of proper access control over sensitive PII increases the risk from insider threats[34] and the potential for breaches, which could lead to identity theft or other forms of consumer fraud against individuals.

Privacy Not Fully Integrated into the FDIC's Risk Management Framework

OMB Circular A-130 requires agencies to implement an RMF that incorporates privacy considerations into the system development lifecycle. According to OMB Circular A-130, the RMF is used to guide and inform the categorization of information and information systems; the selection, implementation, and assessment of privacy controls; and the continuous monitoring of information systems. Therefore, privacy programs play an important role in implementing the RMF. We found that the FDIC did not fully incorporate the privacy considerations described below into the RMF for any of the five systems containing PII that we reviewed. This limited the FDIC's ability to effectively identify, address, and manage privacy risk for its information systems containing PII in a manner consistent with its mission and business objectives.

Categorizing Systems Containing PII

NIST Federal Information Processing Standards (FIPS) Publication 199[35] requires agencies to categorize their information and information systems as "High", "Moderate", or "Low."[36] NIST SP 800-60[37] provides guidelines to assist agencies in categorizing their information and information systems. OMB Circular A-130 states

[33] *See* OIG Report *The FDIC's Information Security Program – 2019* (FDIC OIG AUD-20-001) (October 2019). This audit was conducted pursuant to FISMA, Pub. L. No. 113-283 (codified at 44 U.S.C. § 3551 *et seq*.).
[34] According to FDIC Circular 1600.7, *FDIC Insider Threat and Counterintelligence Program* (September 20, 2016), the term, "insider threat," refers to a threat posed to the FDIC or national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to a Government resource. This threat may include unauthorized disclosure of unclassified sensitive information.
[35] NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004).
[36] These three categories reflect the potential impact to the agency should certain events occur which jeopardize the information and information systems necessary to accomplish the agency's mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
[37] NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008).

that agency SAOPs must review and approve the categorization of systems containing PII in accordance with NIST FIPS Publication 199 and NIST SP 800-60. The SAOP's approval of the system's categorization provides assurance that privacy risks have been adequately considered. At the time of our audit, the FDIC used a standard form, the *Application Security Assessment* (ASA),[38] to determine and document the categorization of its information systems. However, the ASA form did not require the SAOP's review and approval for the categorization of information systems containing PII.

Further, OMB Circular A-130 states that determining the categorization of an information system containing PII "depends on the sensitivity of the PII, the privacy risks, and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation." According to OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular A-123), issued July 2016, the sensitivity level of PII depends on the context, including the purpose of the PII collection.[39] In addition, OMB Circular A-123 states that the agency must consider the volume of PII, because a higher volume of PII about a single individual or individuals may pose increased privacy and other associated risks. However, the ASA form did not address the sensitivity of PII or associated privacy risks as described above, nor explain how FDIC staff considered these privacy factors when determining the categorization of information systems containing PII that we reviewed.

As a result, the FDIC's process may omit consideration of the privacy factors described above that could result in a different categorization level for an information system. For example, an information system that processes a significant volume of PII may pose elevated privacy risk, warranting a categorization of "High." System categorizations are important because they determine the minimum security and privacy controls required to protect the information in the system. Therefore, improper categorization could cause the FDIC not to implement important privacy controls, resulting in non-compliance with Federal privacy requirements or guidance and increased risk of unauthorized access or disclosure of PII.

[38] During the course of our audit, the FDIC replaced the ASA form with a Security Profile document that is now used to determine information system categorization.
[39] OMB Circular A-123 clarifies that the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, how the information will be processed and shared, and the ability to access the information.

Selecting, Implementing, and Assessing Privacy Controls

In April 2013, NIST issued SP 800-53, Revision 4, which introduced an updated catalog of security controls and guidance for Federal information systems. NIST SP 800-53, Revision 4, also included a new appendix containing privacy-related controls (NIST SP 800-53, Appendix J).[40] Some of the privacy controls in NIST SP 800-53, Appendix J, were not new. Rather, they were based on existing privacy laws, regulations, and OMB guidance. For example, a NIST SP 800-53, Appendix J, control recommends that organizations appoint an SAOP and establish a privacy program. In addition, NIST SP 800-53, Revision 4, recommends that agencies assess the implementation of privacy controls in their information systems and programs.[41]

OMB Circular A-130 requires agencies to document their selection of privacy controls from NIST SP 800-53, Appendix J, in system privacy plans, or an equivalent document.[42] These privacy plans describe how agencies implement and assess selected privacy controls. The FDIC did not develop system privacy plans to guide the selection, implementation, or assessment of privacy controls for information systems containing PII that we reviewed.

Further, OMB Circular A-130 requires agency SAOPs to review and approve system privacy plans prior to the system's authorization, reauthorization,[43] or ongoing authorization.[44] The SAOP's approval of the privacy plan affirms that the plan contains appropriate privacy controls to satisfy the privacy and business protection needs of the agency for the associated information system. Because the FDIC had not developed privacy plans or equivalent documents, the FDIC SAOP did not complete these required reviews for the information systems containing PII that we reviewed.

Continuous Monitoring of Privacy Controls

OMB Circular A-130 requires SAOPs to establish and maintain an agency-wide Privacy Continuous Monitoring (PCM) strategy and PCM program. The purpose of the PCM strategy is to identify the privacy controls implemented across the agency

[40] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, Privacy Control Catalogue* (April 2013).
[41] Appendix J states that "[o]rganizations also establish appropriate assessment methodologies to determine the extent to which the privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting designated privacy requirements."
[42] OMB Circular A-130 states that information system security plans and privacy plans may be integrated into a consolidated document.
[43] Reauthorization is a time-driven or event-driven risk determination and risk acceptance decision. For example, if there is a significant change to an information system, a reauthorization may be necessary to review new risks associated with the change.
[44] Ongoing authorization is the risk determination and acceptance decision taken at agreed-upon and documented timeframes in accordance with the agency's mission or business requirements and agency's risk tolerance. For example, if an agency continuously monitors security and privacy controls, identifying no significant risks, continued system operation may be granted.

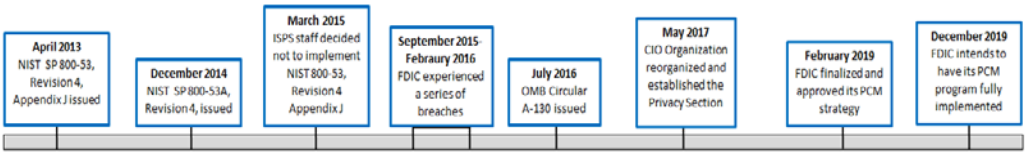
for all information systems containing PII. The PCM strategy further defines the frequency for assessing controls to ensure compliance with applicable privacy requirements and to manage privacy risks. The purpose of the PCM program is to verify the continued effectiveness of selected privacy controls, ensure ongoing awareness of privacy risks, and monitor changes to information systems containing PII.

In July 2018, the FDIC's Privacy Section developed a PCM strategy based on NIST SP 800-53, Revision 5,[45] which had not yet been formally issued by the end of 2018. Therefore, in February 2019, the FDIC revised its PCM strategy to align with the privacy control recommendations contained in NIST SP 800-53, Appendix J. Although the FDIC had developed a PCM strategy, it had not completed the implementation of its PCM strategy for all information systems containing PII. Therefore, the FDIC could not execute its PCM program to continuously monitor privacy controls.

Why the FDIC Did Not Integrate Privacy into the RMF

Based on discussions with Privacy Section staff, the CISO, and the SAOP, we identified two primary causes for the weaknesses we identified (described below). The timeline of events captured in Figure 5 provides context for both causes.

Figure 5: Chronology of RMF Guidance and Implementation



Source: OMB Circular A-130, NIST Publications, and OIG Analysis

First, ISPS staff made a decision in March 2015 not to implement the guidance in NIST SP 800-53, Appendix J, related to the selection and assessment of privacy controls for information systems containing PII. A key reason for this decision was that NIST had not yet developed and issued separate procedures for assessing privacy controls.

In December 2014, NIST issued guidance[46] for assessing the security controls in NIST SP 800-53, Revision 4. However, this guidance did not include procedures for assessing the privacy controls in Appendix J. Instead, the guidance stated that agencies should consult with their SAOPs for guidance on assessing privacy controls

[45] Draft NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (August 2017).
[46] NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (December 2014).

under NIST SP 800-53, Appendix J, until such time as NIST issued procedures for assessing privacy controls.

Second, Privacy Section staff stated that the FDIC diverted considerable resources to address a series of breaches that occurred between 2015 and 2016 wherein departing employees improperly downloaded sensitive PII to removable media devices shortly before leaving the FDIC. The effort to report and address the breaches in 2016 further delayed integration of privacy into the RMF. We previously reported on the lack of sufficient privacy staff resources to respond to these breaches.[47]

In 2017, the FDIC reorganized its privacy staff into the Privacy Section to dedicate staff to perform privacy-related activities. In 2018, the FDIC conducted an assessment of the Privacy Section's workload and its commensurate level of resources. The FDIC's assessment identified resource gaps needed to perform privacy functions. As a result, in 2018, the FDIC approved and funded additional resources, allowing the Privacy Section to direct attention to the privacy requirements established in OMB Circular A-130, Appendix II, including the integration of privacy into the RMF.

In April 2019, the FDIC began to implement its PCM program. As part of the program, the Privacy Section informed us that they had modified procedures and templates used to perform a Privacy Threshold Analysis (PTA)[48] to better address privacy considerations in the categorization of information systems. In addition, Privacy Section staff stated that they were working to revise the FDIC's PIAs to serve as privacy plans. Documentation provided by the Privacy Section demonstrated that they had begun to apply these new procedures and templates on FDIC systems. The FDIC plans to complete the implementation of its PCM program by the end of December 2019.

Absent privacy considerations in the RMF, the FDIC cannot ensure that it is complying with all applicable privacy requirements or effectively managing privacy risks when authorizing its information systems containing PII. For example, an improper system categorization could cause the FDIC not to implement needed privacy controls, exposing individuals to increased risk of harm. Further, not documenting how privacy is considered when determining the categorization of information systems containing PII reduces the FDIC's assurance that its categorization decisions are consistent and adequately supported.

[47] *See* OIG Report, *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (FDIC OIG AUD-17-006) (September 2017).
[48] A PTA is used to determine whether a system involves the collection and use of PII and whether a PIA and/or System of Records Notice is required.

System privacy plans also play an important role in the effective management of privacy risks. Without system privacy plans, assessors cannot conduct efficient or effective privacy control assessments. In addition, the FDIC's CIO, who serves as the Authorizing Official, may not have full knowledge of associated privacy risks and actions for mitigation when authorizing information systems containing PII to operate.

Further, if the FDIC does not regularly monitor privacy controls, it cannot ensure either their continued effectiveness or compliance with applicable statutory and policy requirements, or effectively manage privacy risks. As discussed later in this report, we identified weaknesses in the FDIC's compliance with PII minimization and retention requirements that could have been identified and addressed through the effective implementation of a PCM program. According to OMB Circular A-130, agencies cannot establish an ongoing authorization process for their information systems without a robust and implemented PCM program. Additionally, OMB Circular A-130 states that without effective implementation of the RMF, agencies cannot manage information system-related risks consistent with their mission and business objectives, risk management strategy, and risk tolerance levels established by senior leadership.

Recommendations

We recommend that the CIO/CPO:

1. Revise and implement policies, procedures, and/or guidance to address OMB policy and guidance for assessing privacy risk when categorizing information systems containing PII.

2. Clarify and implement policies, procedures, and/or guidance that defines the role of the SAOP in reviewing and approving system categorizations for information systems containing PII.

3. Develop and approve privacy plans for all information systems containing PII consistent with OMB Circular A-130.

4. Implement a PCM program to regularly assess the effectiveness of privacy controls.

Privacy-Related Roles and Responsibilities Not Adequately Defined or Implemented

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Internal Control Standards) (September 2014) states that management should establish an organizational structure, assign responsibility, and delegate authority to key roles to achieve the entity's objectives. GAO defines a key role as a position in the organizational structure that has been assigned an overall responsibility for the entity.

OMB Memorandum M-16-24, states that, at the discretion of the SAOP, and consistent with applicable law, other qualified agency personnel may perform particular privacy functions assigned to the SAOP. OMB policy emphasizes, however, that the SAOP retains responsibility and accountability for the agency's privacy program. FDIC policies and procedures assigned FDIC Divisions and Offices, and certain individuals, key roles in managing and executing the Privacy Program and records management activities.[49] These key roles include the Deputy CPO; the Privacy Section Chief; the Records and Information Management Governance (RIMGov) Committee; the Corporate Records Officer (CRO); the Chief, RIMU (RIMU Chief); and the Legal Division.

We found that the FDIC did not adequately define the privacy roles and responsibilities for the Deputy CPO. In addition, the FDIC did not implement certain key roles and responsibilities for the RIMGov Committee, the CRO, or the RIMU Chief in support of the FDIC's Privacy Program. Further, the FDIC did not update its privacy policies and procedures to clarify roles and responsibilities subsequent to the reorganization of ISPS in August 2017.

Deputy CPO

In October 2017, the CIO Organization designated the CISO as the Deputy CPO. According to the Privacy Program Plan, the CISO serves as principal advisor for the FDIC's IT Security and Privacy Programs. In this role, the CISO is responsible for developing security and privacy policies, and establishing and managing the FDIC Privacy Program.

The Privacy Program Plan, however, does not provide any information regarding how the individual serving in this role supports the SAOP in managing the Privacy Program. In addition, FDIC Directive 1360.20 does not acknowledge the FDIC's establishment of the Deputy CPO role and related roles and responsibilities. In

[49] These policies and procedures include FDIC Directive 1360.20, *Privacy Program*, Circular 1210.1, *FDIC Records and Information Management Policy Manual,* and the FDIC's Privacy Program Plan.

November 2018, we brought our concerns regarding the lack of defined roles and responsibilities to the Deputy CPO's attention. The Deputy CPO acknowledged that the FDIC had not fully defined or established in policy the roles and responsibilities for the position.

According to GAO's *Standards for Internal Control in the Federal Government*, defining roles and responsibilities in policies and procedures is an important control for ensuring the effective implementation of any Federal program. Defined roles and responsibilities would provide the individual serving as Deputy CPO a proper understanding of required duties and management's expectations, and provide the necessary authority to implement those duties across the FDIC. Defined roles and responsibilities also allow management the ability to effectively monitor and evaluate the activities of the Deputy CPO.

RIMGov Committee

In June 2015, the FDIC established the RIMGov Committee to oversee records management implementation and compliance across the FDIC (including records containing PII). FDIC Circular 1210.1, *FDIC Records and Information Management (RIM) Policy Manual* (RIM Policy Manual) (June 2016) assigns the RIMGov Committee responsibility for providing strategic direction, guidance, and approval for RIMU initiatives and for helping to raise support for records management activities among FDIC Divisions and Offices. According to its charter, the CRO leads the RIMGov Committee, and its members include representatives from various FDIC organizational components, such as privacy staff, security staff, and FDIC business Divisions and Offices. The charter also states that the RIMGov Committee has responsibility for:

- Assessing the effectiveness of the FDIC's records management policies, business processes, information repositories, and technologies;
- Overseeing and recommending revisions to the RRS in accordance with Federal laws and regulations, and the FDIC's business needs;
- Reducing legal costs and risk by automating the disposal of information (including PII) that is of low value and unnecessary; and
- Disseminating relevant records management information to and from the RIMGov Committee to senior management and employees in the FDIC's Divisions and Offices.

The RIMGov Committee disbanded in 2016, when the former CRO left her position. The current CRO stated that the RIMGov Committee's roles and responsibilities had not been transferred to another group. Although the CRO has responsibility for

overseeing FDIC-wide records management efforts, she pointed out that the lack of a governance body diminished her ability to enforce record retention and disposal requirements throughout the FDIC.

CRO and RIMU Chief

RIMU provides advice and support to the Privacy Program to help ensure that records containing PII comply with the RRS. The RIM Policy Manual (Manual) identifies two key roles as it relates to RIMU—the CRO and RIMU Chief—and defines different responsibilities for each. According to the Manual, the CRO is responsible for overseeing RIMU; reviewing and approving RIM policies, procedures, and processes; and approving all changes to the RRS. The RIMU Chief provides direct supervision to RIMU staff and reports on the progress of RIM activities to the CRO. The RIMU Chief is also responsible for conducting an annual compliance evaluation of the RIM Program against program objectives and criteria, including the RRS. The individual serving as RIMU Chief has served as the CRO since 2016.[50]

We found that the CRO/RIMU Chief did not perform annual compliance evaluations against stated program objectives and criteria as required by the Manual. These evaluations are intended to help ensure that FDIC Divisions and Offices adhere to the RRS by disposing of records in a timely manner, and obtaining approval from the CRO when they have a business need to deviate from the RRS. The CRO/RIMU Chief stated that RIMU did not conduct these evaluations because they did not have enough resources and had not provided the necessary "tools" to the Divisions and Offices to help ensure compliance with records management requirements. Such tools include RIM training for all FDIC employees, an automated tool with which to create File Plans, and other technical capabilities.

As described in our finding entitled, *Minimization of PII Records Not Effectively Implemented,* we found that FDIC Divisions and Offices did not always comply with the RRS or obtain approval from the CRO for deviations from the RRS. The CRO/RIMU Chief stated that annual compliance evaluations would be conducted once FDIC Divisions and Offices had the needed tools and resources to manage records electronically. During our audit, the CRO/RIMU Chief provided guidance and began implementing the automated RSS tool to help FDIC Divisions and Offices establish File Plans.

[50] We refer to the positions of RIMU Chief and CRO hereinafter as the CRO/RIMU Chief.

Key Organizational Change

FDIC Directive 1360.20 assigns various responsibilities to ISPS on behalf of the SAOP. These responsibilities include managing the Privacy Program to address legal, regulatory, privacy, and information policy issues; providing privacy training to employees and contractors; managing privacy complaints and inquiries; collaborating with senior management to address non-compliance with privacy requirements; and overseeing the PIA process.

As previously discussed, in 2017, the FDIC re-organized ISPS by separating its Privacy Section and Security and Compliance Sections into separate component offices under the OCISO. However, the FDIC did not update its Directive 1360.20 and related policies and procedures to clarify the roles and responsibilities of these respective offices. Providing this clarification is important to help ensure that individuals and component offices supporting the SAOP in managing the Privacy Program carry out their privacy responsibilities in a consistent, repeatable, and accountable manner.

Impacts of Roles and Responsibilities Not Being Defined or Executed

The lack of current, clearly defined, and consistently executed roles and responsibilities of the SAOP and agency personnel supporting the SAOP limited the FDIC's ability to satisfy privacy requirements and Privacy Program objectives. As described in this report, we found that the SAOP and supporting component offices were not fulfilling key responsibilities regarding the Privacy Program. We determined that the FDIC did not:

- Fully integrate privacy into the FDIC's RMF, including the development and implementation of a Privacy Continuous Monitoring (PCM) program;
- Effectively manage and secure PII records stored in network shared drives and in hard copy;
- Minimize its PII holdings by managing records in accordance with established records retention and disposition schedules; or
- Ensure that PIAs were always completed, monitored, and retired in a timely manner.

Recommendations

We recommend that the CIO/CPO coordinate with the Chief Operating Officer (COO) to:

5. Update policies and/or procedures to reflect the current organizational structure of the Privacy Program and responsibilities of agency personnel and component offices that support the FDIC's Privacy Program.

6. Establish a governance body or other governance mechanisms to assist the CRO with records management implementation and compliance.

PII Not Effectively Managed

OMB Circular A-130 requires agencies to maintain an inventory of information systems[51] containing PII. OMB Circular A-130 also requires agencies to regularly review all PII maintained by the agency to ensure compliance with privacy requirements. This requirement applies to PII in any form or medium, including hard copy and electronic media. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (April 2010), similarly recommends that organizations identify all PII residing in their environment, including PII in databases, network shared drives, backup tapes, and contractor sites. According to NIST SP 800-122, organizations cannot properly protect PII of which they are unaware.

As of June 11, 2018, the FDIC reported that it maintained 338 information systems containing PII and managed an inventory of 174 information systems containing sensitive PII. However, the FDIC did not effectively manage sensitive PII stored in network shared drives and in hard copy. Therefore, the FDIC did not regularly review this PII to ensure compliance with privacy requirements. In addition, we identified sensitive PII stored in network shared drives and in hard copy that the FDIC did not properly secure, increasing the risk from insider threats and potential data breaches.

PII Stored in Network Shared Drives

FDIC policy allows employees and contractors to store business records, including records containing PII, on the FDIC's internal network shared drives.[52] According to the Division of Information Technology (DIT) Infrastructure Services Branch, the FDIC maintained over 200 resource servers on its internal network that were capable

[51] OMB Circular A-130 defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[52] *See* the RIM Policy Manual Chapter 8.

of supporting network shared drives. Each of these shared drives can store a significant amount of information. For example, we observed one network shared drive that contained over 35,000 folders.

We reviewed a judgmental sample of six network shared drives and found that they contained unsecured sensitive PII on FDIC employees and customers of failed banks. Such PII included FDIC employee personnel actions; employee performance appraisals; and both employee and bank customer credit information that included names, addresses, and SSNs. On June 7, 2019, we issued an Advisory Memorandum to the CIO and CISO describing our concerns. *See* Appendix 6 for our Advisory Memorandum.

On June 21, 2019, the CIO Organization responded with a description of its plans to address these concerns. Specifically, the CIO Organization planned to perform automated scans of the internal network to identify unsecured sensitive information, including PII; complete actions to protect any unsecured sensitive information; and develop a long-term strategy for storing sensitive data. The CIO Organization planned to complete these actions by the end of calendar year 2019. *See* Appendix 7 for the CIO Organization's response. On August 8, 2019, the CIO reported that the OCISO had scanned all network shared drives and identified 986 instances in which sensitive information, including sensitive PII, may not be properly secured. The CIO was working to remediate these issues at the close of our audit.

PII in Hard Copy

The FDIC maintained a significant quantity of hard copy PII in its facilities and off-site storage locations. For example, the FDIC maintained 3,790 hard copy FOIA case files within its Legal Division offices. Based on FDIC documentation and our direct inspection of these records, FOIA case files contain sensitive PII on individual requestors such as full names, addresses, state identification numbers, financial information, and SSNs.

As part of a separate audit of the FDIC's Information Security Program,[53] our office conducted unannounced walkthroughs of selected FDIC areas within the FDIC's Virginia Square facility. The purpose of these walkthroughs was to identify portable storage media, such as CDs and DVDs, as well as hard copy sensitive information, including PII, that may not be properly secured in accordance with FDIC policy and guidance.[54] We identified significant quantities of sensitive hard copy information, including sensitive PII, that was accessible to anyone in the facilities we reviewed,

[53] *See* OIG Report *The FDIC's Information Security Program – 2019* (FDIC OIG AUD-20-001) (October 2019).
[54] FDIC Circular 1360.9, *Protecting Sensitive Information*, (October 2015) states that only individuals who have a legitimate need to access sensitive information in the performance of their duties may be provided access. FDIC Circular 1360.9 requires hard copy sensitive information to be stored in corporate facilities, such as locked drawers, file cabinets, and file rooms whenever possible.

including employees, visitors, and contractor personnel. The majority of unsecured sensitive PII we found was stored in unlocked filing cabinets and boxes in building hallways. Examples included Suspicious Activity Reports (SAR)[55] on individuals, tax returns, FOIA case files, and documents containing employee names, SSNs, and dates of birth. We reported the results of our walkthroughs, along with recommendations to better safeguard sensitive hard copy information stored in FDIC facilities, in our annual FISMA audit report on the FDIC's Information Security Program.

Limitations and Impacts of Not Managing PII in Network Shared Drives and in Hard Copy

The Privacy Act and OMB policy require agencies to safeguard sensitive PII from unauthorized access or disclosure. Ineffective management of PII stored on the FDIC's internal network and in hard copy allowed weaknesses in access controls over this information to go undetected. The lack of proper access controls made this information vulnerable to theft from an insider, increasing the risk of a breach. A breach could result in identity theft or other forms of consumer fraud against individuals, and expose the FDIC to unnecessary costs and potential legal liability.

A key reason why the FDIC did not effectively manage (track or regularly review) PII stored in network shared drives and in hard copy was that it did not implement a uniform method to categorize and label its data, including PII. The CIO Organization's security architecture documentation recognized this limitation when it stated that "[t]here is no centralized data tagging done at the organizational level, making it impossible to monitor specific information such as PII."[56]

In late 2016, the FDIC initiated its Data Protection Program (DPP). The purpose of the DPP is to provide the FDIC with standards, policies, support, and methods to identify, categorize, label, and protect PII and sensitive information. The DPP will help to identify where PII resides within the FDIC's environment. According to the DPP Charter, the FDIC will use tools, policies, and procedures to manage and enforce data protection and compliance on an ongoing basis. At the close of our audit field work, the FDIC had completed draft documents relating to a data protection policy directive, labeling guide, and associated job aids to help FDIC employees and contractor personnel label data, including PII. However, the FDIC had not issued these documents in final form, distributed them to agency personnel, or implemented them.

[55] Banks file SARs with the Financial Crimes Enforcement Network, a bureau of the Department of the Treasury, when they detect known or suspected criminal violation of federal law, a suspicious transaction related to money laundering activity, or a violation of the Bank Secrecy Act. A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to money laundering or terrorist activity. Federal law (31 U.S.C. 5318(g)(2)) prohibits the notification of any person that is involved in the activity being reported on a SAR that the activity has been reported. Financial Crimes Enforcement Network guidance explains that this prohibition effectively precludes the disclosure of a SAR or the fact that a SAR has been filed to anyone.
[56] OCISO's *Security Architecture—Application Security and Data Protection* document (March 26, 2018).

The FDIC should categorize and label PII stored in network shared drives and in hard copy to identify where it resides within its records management environment. When information is not categorized or labeled, the FDIC cannot ensure that it is effectively monitoring PII within its environment and complying with privacy laws, regulations, policy, and guidelines. This includes ensuring that proper access controls are in place to allow access to only those who need the PII to perform their official duties.

Recommendations

We recommend that the CIO/CPO:

7. Complete and implement the data protection program policy directive, data labeling guide, and associated job aids.

8. Develop and implement controls to ensure that PII stored in network shared drives and in hard copy is regularly monitored and reviewed for compliance with privacy laws, regulations, policy, and guidelines.

Minimization of PII Records Not Effectively Implemented

OMB Circular A-130 requires agencies to reduce their PII holdings to the minimum amount necessary for the proper performance of authorized agency functions. This concept, referred to as "Minimization," is a Fair Information Practice Principle (FIPP), recognized in Federal requirements.[57] The principle of Minimization states that organizations should (1) only collect, use, and maintain PII that is directly relevant and necessary to accomplish a legally authorized purpose and (2) only retain PII for as long as is necessary to accomplish that purpose. Based on this principle, OMB Circular A-130 requires agencies to maintain and dispose of records containing PII in accordance with applicable records retention and disposition schedules.

Consistent with OMB policy requirements, the FDIC established a RIM Policy Manual to govern the creation, management, use, and disposition of business records and information, including PII, that the FDIC creates and receives in the course of conducting business. The RIM Policy Manual requires Divisions and Offices to retain and destroy business records and information in accordance with the FDIC's RRS and any applicable legal holds.[58] The RRS defines the required retention and

[57] According to OMB, the FIPPs are a collection of widely accepted principles that agencies should use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FDIC recognizes its obligation to the FIPPs in its Privacy Program Plan.
[58] The FDIC Legal Division may issue a written legal hold notice to inform appropriate FDIC employees and contractors of records and information that must be retained until a legal matter is resolved. Records subject to legal hold must be preserved and should not be altered, modified, discarded, or destroyed.

disposal periods for FDIC business records, including those that contain PII.[59] According to the RIM Policy Manual, retention periods in the RRS are based on applicable laws, rules, regulations, and FDIC business needs. For example, the Federal Deposit Insurance Act requires the FDIC, as receiver for a failed financial institution, to maintain an institution's records (that are fewer than 10 years old as of the date of appointment) for at least 6 years. These records are eligible for destruction after this required retention period, unless such destruction is prohibited by a court, Government agency, or law.[60] The RRS requires the FDIC to destroy or delete these records 6 years after appointment as receiver.

The FDIC did not dispose of PII within the timeframes established in the RRS for three of five information systems we selected for review. Specifically, the FDIC did not:

- Dispose of electronic or hard copy failed bank records that exceeded the retention period in the RRS.[61] These records pertained to 391 failed financial institutions.

- Dispose of 3,790 hard copy and another 2,544 electronic FOIA records that no longer served a business need.[62]

- Dispose of approximately 13,800 records stored in the Background Investigation Database System (BIDS) that exceeded the retention period in the RRS.[63]

Appendix 5 provides detailed information regarding these three deficiencies.

Why PII Minimization Was Not Implemented

We found that the FDIC did not implement three key controls defined in the RIM Policy Manual. These controls were intended to ensure business records and information, including PII, are disposed of in accordance with the RRS. The lack of implementation for these three controls reduced the FDIC's ability to dispose of records containing PII in a timely manner.

(1) File Plans Not Managed. The RIM Policy Manual states that compliance with the retention periods specified in the RRS is typically accomplished by establishing File Plans. The RIM Policy Manual also states that all business records must be

[59] The RRS classifies business records based on their content, describes the records, and applies a retention period and disposal instructions. Extensions to retention periods must be approved in writing by RIMU.
[60] 12 U.S.C § 1821(d)(15)(D).
[61] The FDIC stores electronic failed bank records in the FDIC Business Data Services (FBDS) system. The Division of Resolutions and Receiverships (DRR) manages FBDS.
[62] The FDIC stores electronic FOIA records in the FOIA system. The Legal Division manages the FOIA system.
[63] The FDIC stores electronic background investigation information on bank directors, officers, and other employees in BIDS. The Division of Risk Management Supervision (RMS) manages BIDS.

managed according to the FDIC RRS and appropriate guidelines, procedures, and File Plans. File Plans contain instructions for the retention and disposition of documents stored in repositories.[64] In addition, File Plans identify associated information for FDIC records, such as the record title, record description, media type (electronic or hard copy), location (network shared drive or file room), and disposition instructions. Division and Office Record Liaisons facilitate the timely disposition of inactive business records (paper and electronic) and non-record material in accordance with the File Plans. However, we determined that Divisions and Offices responsible for three of the five information systems we selected for review had not finalized their File Plans.

During our audit, RIMU developed an automated tool for FDIC Divisions and Offices to use when creating and finalizing File Plans. RIMU centrally manages File Plans using this tool in coordination with Division and Office Record Liaisons. At the close of our field work in April 2019, 8 of 18 FDIC Divisions and Offices had initiated or completed File Plans using this tool. Without implementing this key control, the FDIC has reduced assurance that Divisions and Offices will track and dispose of PII within the timeframes established in the RRS.

(2) Compliance Reporting Not Performed. The RIM Policy Manual requires DIT to "generate appropriate reports for monitoring and auditing of compliance with records retention and disposition requirements for electronically stored information in accordance with the RRS and any applicable File Plans." However, the RIM Policy Manual does not prescribe the content of reports that DIT must generate, the frequency of those reports, or who should receive and monitor such reports. In addition, DIT did not generate these reports for the five information systems we reviewed.

According to the Deputy Director, Delivery Management Branch, DIT, at the time the five systems in our sample were developed, the FDIC had not yet established a requirement to implement automated retention controls. Therefore, DIT did not generate the required reports for these systems. Without implementing this key control, the FDIC cannot ensure that its information systems dispose of PII within the timeframes established in the RRS.

(3) Annual Program Evaluations Not Conducted. The annual evaluations assess compliance against the program's objectives and criteria, including compliance with the RRS. As previously discussed, the RIMU Chief stated that RIMU did not perform annual program evaluations. Without these evaluations, the RIMU Chief cannot

[64] According to the RIM Policy Manual, the term, "repository," applies to systems, network locations, or application data stores where electronic documents and data are kept during active use or archival storage. The term can also refer to a place where hard copy records are stored.

verify that Divisions and Offices dispose of records, including records containing PII, within the timeframes established in the RRS.

Implementing the principle of Minimization reduces privacy risk. According to NIST SP 800-122, an organization can significantly reduce the likelihood of harm caused by a breach if it minimizes the amount of PII it uses, collects, and stores. Maintaining sensitive PII beyond the minimum retention periods defined in the RRS, without justification, exposed the FDIC to unnecessary risk of a breach.

During our audit, the FDIC drafted a RIM Framework for its information systems, including systems containing PII. The purpose of the RIM Framework is to ensure that all FDIC information systems, applications, and services that capture, create, or maintain FDIC business records comply with records management policies and procedures. However, the FDIC had not finalized and implemented the RIM Framework.

Recommendations

We recommend that the COO:

9. Ensure that Divisions and Offices complete File Plans.

10. Perform annual evaluations of the RIM program.

We recommend that the CIO/CPO coordinate with the Deputy Director, Corporate Services Branch, DOA to:

11. Generate reports to monitor and audit compliance with the FDIC's records retention and disposition requirements.

We recommend that the Deputy Director, Corporate Services Branch, DOA, coordinate with the CIO/CPO to:

12. Finalize and implement a records management framework for FDIC information systems that ensures compliance with records retention requirements.

Effectiveness of PIA Process Needed Improvement

In general, the E-Gov Act requires Federal agencies to conduct PIAs before developing or procuring IT that collects, maintains, or disseminates PII. The statute also requires agencies to conduct PIAs before initiating a new collection of information that will be maintained and disseminated using IT. The statute further requires agencies to make PIAs publicly available, if practicable.[65] OMB has issued a policy and related guidance to assist agencies in implementing the privacy provisions of the E-Gov Act, including provisions related to PIAs.[66] Notably, OMB policy requires agencies to regularly update PIAs in order to ensure that they remain current.

The FDIC established a policy and implemented a process for conducting and posting PIAs. However, the FDIC did not always complete, monitor, or retire PIAs in a timely manner. Specifically, the FDIC did not:

- Finalize PIAs for 4 of its 174 information systems containing sensitive PII before authorizing the systems to operate.

- Routinely review, update, or remove PIAs on its public website. For example, we found that the FDIC did not remove nine PIAs that related to systems that had already been retired.

Our previous OIG audit report on the FDIC's Privacy Program (September 2011) similarly identified instances in which the FDIC did not make PIAs available to the public until after the FDIC began collecting the PII.[67] In response, the FDIC issued its Circular 1360.19, *Privacy Impact Assessment Requirements* (2012, and updated in August 2016). FDIC Circular 1360.19 defines high-level policy, guidance, and responsibilities for managing PIAs, and includes a requirement that PIAs be made publicly available before the FDIC collects, maintains, or disseminates PII.

However, FDIC Circular 1360.19 and other FDIC policies and procedures did not identify the requirement to complete a PIA as an important step in the system authorization process.[68] The system authorization process includes a review of key documents, such as the system security plan, system privacy plan, and plans of

[65] The statute provides that agencies may determine to not publicly post a PIA for security reasons, or to protect classified, sensitive, or private information contained in the PIA. *See* E-Gov Act, § 208(b)(1)(C).
[66] *See* OMB Circular A-130 and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
[67] *See* OIG Report, *The FDIC's Privacy Program- 2011*, (AUD-11-014) (September 2011).
[68] OMB Circular A-130 requires agencies to authorize their information systems to operate. A senior management official (the Authorizing Official) reviews information describing the security and privacy posture of an information system, and using that information, determines whether the risk to mission/business operations is acceptable. If the Authorizing Official determines that the risk is acceptable, then the official explicitly accepts the risk.

actions and milestones,[69] before authorizing a system to operate. Further, FDIC Circular 1360.19 and other FDIC policies also did not define:

- Requirements for periodically reviewing PIAs to ensure they remain accurate and are removed from the public website when the associated systems are retired;[70] and

- Timeframes for posting revised PIAs to the FDIC's public website.

When the FDIC does not complete PIAs in a timely manner or maintain accurate and up-to-date PIAs on its website, it cannot ensure compliance with the E-Gov Act and OMB policy, and it cannot ensure that the privacy rights of individuals are adequately protected. Further, untimely publication of PIAs reduces transparency and accountability to the public.

As described earlier in this report, the Privacy Section began implementing the PCM program during our audit. The PCM program will help ensure that PIAs remain current. Privacy Section staff stated that they plan to complete implementation of the PCM program by December 2019.

Recommendations

We recommend that the CIO/CPO:

13. Revise and implement processes to ensure that PIAs are completed and made available to the public prior to authorizing information systems containing PII to operate.

14. Revise and implement policy and/or processes to ensure PIAs are periodically reviewed, updated, and removed from the FDIC's public website when systems are retired.

[69] Plans of actions and milestones are used to document tasks that need to be accomplished. They detail resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.
[70] OMB and NIST do not define timeframes for reviewing PIAs. However, OMB Circular A-130 states a PIA should be considered a living document that agencies must update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.

FDIC COMMENTS AND OIG EVALUATION

The FDIC provided a written response, dated December 16, 2019, to a draft of this report. The response is presented in its entirety in Appendix 8. The FDIC concurred with all 14 of the report's recommendations. The recommendations will remain open until we confirm that corrective actions have been completed and are responsive. Appendix 9 contains a summary of the FDIC's corrective actions.

Objective

The objective of the audit was to assess the effectiveness of the FDIC's Privacy Program and practices. We assessed effectiveness of the FDIC's Privacy Program controls, such as policies and procedures, roles and responsibilities, and awareness training, by evaluating compliance with selected requirements in privacy-related statutes, OMB policy and guidance, and NIST guidance where applicable. We also assessed the effectiveness of the FDIC's privacy practices by determining whether they complied with FDIC policy, procedures, and guidance, as well as selected requirements in privacy-related statutes, OMB policy and guidance, and NIST guidance where applicable.

We conducted this performance audit 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Except as noted in the report, our findings and conclusions are as of April 22, 2019.

Scope and Methodology

To address the audit objective, we:

- Reviewed the FDIC's Privacy policies and procedures to determine their compliance with current Federal laws and regulations governing privacy.
- Reviewed FDIC-generated reports describing PII inventories, network shared drives, and hard copy records.
- Examined FDIC reports and responses regarding its compliance with privacy-related requirements.
- Interviewed FDIC officials with privacy responsibilities, including the SAOP, the CISO, select Privacy Section staff, Legal Division officials, the CRO/RIMU Chief, record liaisons, and other officials with privacy responsibilities, to determine whether:
    - Obsolete technologies in the FDIC's IT environment impaired the FDIC's ability to manage and protect PII in accordance with Federal requirements;

- The FDIC implemented the DPP, including data categorization and labelling, to ensure the identification and protection of PII in both hard copy and electronic formats;

- The FDIC fulfilled its privacy roles and responsibilities in accordance with Federal law, regulation, and FDIC-specific requirements; and

- FDIC employees and Divisions and Offices adhered to roles and responsibilities relating to record retention and file management for both hard copy and electronic PII.

We relied on computer processed information to conduct our analysis of PII inventories and PII stored outside of designated systems containing PII. We corroborated this information to support our audit conclusions with other information from various sources, including direct examination, supporting documentation, and testimonial evidence from subject matter experts. As a result, we determined that the information was sufficiently reliable for the purposes of our audit.

As part of our work, we obtained an inventory of 174 FDIC and contractor-owned information systems containing sensitive PII. We judgmentally selected five of these systems to determine the effectiveness of system-specific privacy controls. The selected systems were FBDS, BIDS, FDICconnect, FOIA, and the Personnel Security Records application. We selected these systems because they contained sensitive PII and support mission-essential functions, such as supervising insured financial institutions, managing failed financial institutions, and protecting depositors of insured financial institutions. We also selected these systems in order to obtain representation from multiple FDIC Divisions. We assessed each system to determine whether:

- PIAs were completed before system authorization, published in a timely manner, and contained required elements.

- System authorization documentation addressed privacy considerations; a system privacy plan was in place; and whether the FDIC tested and monitored privacy controls.

- System owners provided access only to authorized individuals and further removed access as required.

- System users completed privacy awareness training, role-based training (based on responsibility/access level), and signed/agreed to rules of behavior for system use.

- System controls or Divisions and Offices enforced compliance with the FDIC's RRS.

- Contracts (if applicable) included clauses addressing privacy requirements and reflected current Federal requirements and guidelines for outsourced systems.

- Breaches involving PII occurred and whether system controls failed to prevent any breaches (weaknesses in access controls, training, etc.).

Our audit approach was largely based on the requirements set forth in OMB Circular A-130. OMB Circular A-130 establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services. OMB Circular A-130, Appendix II, organizes key privacy responsibilities and requirements for Federal agencies managing information resources into nine areas. We assessed compliance for selected responsibilities and requirements in eight of the nine control areas. Appendix 2 provides additional information regarding our assessments.

Table 2 identifies key privacy requirements contained in OMB Circular A-130, Appendix II, and our assessment of effectiveness for each. Table 2 does not represent a comprehensive listing of all privacy controls contained in OMB Circular A-130, Appendix II, or all of the controls and practices that we assessed.

Table 2: OIG Assessment of Selected Privacy Requirements in OMB Circular A-130

Requirement/Responsibility	Assessment of Effectiveness
1. General Requirements	
Establish and maintain a comprehensive privacy program.	Effective
*Ensure compliance with privacy requirements and manage privacy risks.	The FDIC issued policies and procedures to ensure compliance with the majority of applicable statutory, regulatory, and policy privacy requirements. However, FDIC policies and procedures related to the RMF and managing privacy risks were not adequate, and other policies involving privacy were not always adhered to and/or were outdated. In addition, the FDIC designated key roles and supporting positions for managing and executing the Privacy Program. These included the Deputy CPO, RIMGov Committee, and CRO/RIMU Chief. However, these roles and their associated responsibilities were not either adequately implemented or defined in policy.
Develop and maintain a privacy program plan.	Effective
Designate a Senior Agency Official for Privacy.	Effective
Incorporate privacy requirements into the enterprise architecture.	Effective
	Partially Effective
2. Considerations for Managing PII	
Maintain an inventory of agency information systems that involve PII.	Effective
*Regularly review and reduce PII to the minimum necessary.	The FDIC did not track or regularly review PII stored outside of its information systems containing PII. Additionally, PII in electronic format and hard copy was not adequately secured.
*Follow approved RRSs for records with PII.	The FDIC did not always comply with its RRS for PII retention and disposal or adhere to PII minimization principles for three of the five systems we reviewed.
	Partially Effective
3. Budget and Acquisition	
Identify and plan for resources needed for the privacy program.	Effective
Establish a process to evaluate privacy risks for IT investments.	Effective
Upgrade, replace, or retire unprotected information systems.	Effective
	Effective

4. Contractors and Third Parties	
Ensure that contracts and other agreements incorporate privacy requirements.	Effective
Maintain an inventory of contractor information systems.	Effective
	Effective
5. Privacy Impact Assessments	
*The E-Government Act requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.	The FDIC established a policy and implemented a process for conducting and posting PIAs. However, the FDIC did not finalize PIAs for 4 of its 174 information systems containing PII before the systems were authorized. Further, the FDIC did not remove PIAs from its public website for nine retired systems.
PIAs must describe the PII that is being collected; why the PII is being collected; its intended use; with whom it will be shared; opportunities individuals have to decline providing this information; how it will be secured; and whether a System of Records Notice is being created.	Effective
	Partially Effective
6. Workforce Management	
Develop a set of privacy competency requirements.	Effective
Ensure that the workforce has the appropriate knowledge and skills.	Effective
	Effective
7. Training and Accountability	
Maintain agency-wide privacy training for all employees and contractors.	Effective
Ensure that privacy training is consistent with applicable policies.	Effective
Provide role-based privacy training to appropriate employees and contractors.	Effective
Ensure that employees and contractors read and agree to rules of behavior.	Effective
	Effective
8. Incident Response	
The audit did not include an assessment of the Privacy Program's incident response function as this control area was assessed in previous OIG audits.	
9. Risk Management Framework	
*Implement a risk management framework to manage privacy risks.	The FDIC adopted the NIST RMF, but did not fully integrate privacy into this framework as prescribed by OMB Circular A-130.

*Ensure that the SAOP reviews and approves the categorization of information systems that involve PII.	The SAOP did not review and approve the categorization of information systems containing PII. Further, the FDIC's security categorization form did clearly define how PII considerations are used to (1) determine impact levels, specifically as they relate to PII confidentiality impact, or (2) reach an overall security categorization for the system.
*Agencies shall select security and privacy controls for each information system.	The FDIC did not select privacy controls for any of the five systems we sampled.
*Develop, approve, and maintain privacy plans for information systems.	The FDIC did not develop, approve, or maintain privacy plans for any of the five systems we sampled.
*Establish and maintain a privacy continuous monitoring program.	The FDIC established a PCM strategy during the course of our audit. However, the FDIC had not implemented its PCM program to execute the strategy.
	Not Effective

* Indicates an area of non-compliance.

Source: OMB Circular A-130, Appendix II, and OIG Analysis.

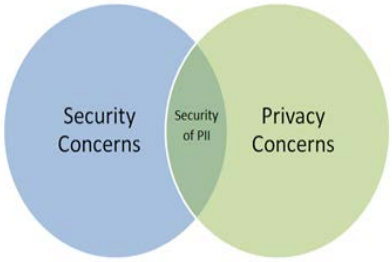
Acronyms and Abbreviations

ASA	Application Security Assessment
BIDS	Background Investigation Database System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPO	Chief Privacy Officer
CRO	Corporate Records Officer
DIT	Division of Information Technology
DOA	Division of Administration
DPP	Data Protection Program
DRR	Division of Resolutions and Receiverships
ERM	Enterprise Risk Management
FBDS	FDIC Business Data Services
FDIC	Federal Deposit Insurance Corporation
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
GAO	Government Accountability Office
ISPS	Information Security and Privacy Staff
IT	Information Technology
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCM	Privacy Continuous Monitoring
PIA	Privacy Impact Assessment
PTA	Privacy Threshold Analysis
PII	Personally Identifiable Information
RIM	Records Information Management
RIMGov	Records and Information Management Governance
RIMU	Records and Information Management Unit
RMF	Risk Management Framework
RMS	Division of Risk Management Supervision
RRS	Records Retention Schedule
SAOP	Senior Agency Official for Privacy
SAR	Suspicious Activity Report
SP	Special Publication
SSN	Social Security Number

Relationship Between Security and Privacy

According to OMB Circular A-130 and NIST,[71] it is important to understand the relationship—and particularly the distinctions—between information security and privacy. NIST SP 800-37, Revision 2, states that information security focuses on protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction. Privacy focuses on ensuring compliance with applicable privacy requirements and managing the risks associated with the collection, use, dissemination, storage, maintenance, disclosure, or disposal of PII. Figure 6 illustrates the interrelationship between privacy and information security.

Figure 6: Relationship Between Security and Privacy



Source: NISTIR 8062

When an information system processes PII, both the organization's information security program and privacy program have a shared responsibility for managing potential risks. According, to NISTIR 8062, there are security concerns unrelated to privacy just as there are privacy concerns unrelated to security. For example, security tools can create privacy concerns about the degree to which information is revealed about individuals that is unrelated to cybersecurity.

According to NIST SP 800-37, Revision 2, because information security and privacy involve distinct issues, concerns, and requirements, they often require different expertise to effectively address. Notwithstanding these distinctions, NIST SP 800-37, Revision 2, recognizes that information security and privacy are related due to their complementary objectives of managing PII. Therefore, OMB Circular A-130 recommends that agencies take a coordinated approach when identifying and managing security and privacy risks and complying with applicable requirements.

[71] *See* NIST Special Publication (SP) 800-37, Revision 2, and NIST Interagency or Internal Reports (NISTIR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* (January 2017).

We judgmentally selected five information systems containing sensitive PII to review each system's compliance with established records retention codes. We determined that three of the systems maintained records beyond the established retention period in the RRS. Below we provide a summary of each non-compliant system.

FDIC Business Data Services (FBDS) System

DRR maintains failed bank records in both hard copy format at Iron Mountain facilities[72] and in electronic format within FBDS. These records contain sensitive PII, such as full names, SSNs, birthdates, financial information, criminal information, and investigative reports on failed bank borrowers, customers, complainants, claimants, guarantors, creditors, and officers. According to the RIM Policy Manual, records of failed insured depository institutions are eligible for destruction 6 years after the FDIC is appointed receiver, unless such destruction is prohibited by a court, Government agency, or law. The RRS requires that the FDIC destroy or delete these records 6 years after appointment as receiver.

According to RIMU officials and results from our review of the FDIC's litigation actions, records eligible for destruction included failed bank records for 391 institutions. These institutions failed between January 2009 and December 2012 and exceeded the 6-year retention period. Based on reports from RIMU and DRR officials, we determined that failed bank records exceeding the retention requirement consisted of 67,338 boxes of hard copy records stored at offsite facilities maintained by an external storage provider and another 260 terabytes of data in electronic format in FBDS.[73]

Freedom of Information Act System (FOIA)

The FOIA system is a commercial off-the-shelf application managed by the Legal Division that automates compliance with record access and disclosure requirements under the Freedom of Information Act. Individuals and organizations submit FOIA requests to the FDIC, and the FDIC creates an electronic file whose content is responsive to each request. These electronic files may contain multiple references to sensitive PII, including full name, SSNs, birth dates, employment records, medical information, and legal documents.

According to the RRS, the FDIC should destroy FOIA records 6 years after fulfillment or denial of the associated FOIA request. We identified 158 boxes containing 3,790

[72] FDIC contracts with Iron Mountain, Inc. for a range of records management and storage services, including records destruction.
[73] The FDIC Legal Division piloted a tool to support the legal hold review process for failed bank data during our audit. As a result, the amount of records exceeding FDIC-established retention periods may be reduced.

FOIA files stored in a locked file room beyond their retention period of 6 years.[74] We also found that 2,544 of the 5,605 electronic files (45 percent) in the FOIA system were over 6 years old. In response to our findings, the Legal Division either destroyed or deleted these records.

Background Investigation Database System (BIDS)

RMS uses BIDS to conduct background investigations on potential bank directors, officers, and principals in connection with applications and notices submitted to the FDIC. BIDS records contain sensitive PII for these individuals, including full names, SSNs, addresses, employment records, investigative reports, and criminal history information.

According to the RRS, the FDIC should destroy such records 5 years after they are submitted to the FDIC for review. However, the BIDS PIA stated that RMS had requested that records in the system be maintained for up to 50 years. This extended period exceeded the maximum retention period approved by RIMU for any FDIC business record.[75] Further, the CRO/RIMU Chief had not approved RMS's request for a 50-year retention period for BIDS records.

During our audit, we brought this matter to the attention of RMS officials. RMS subsequently drafted a revised PIA and applied a 30-year retention period for BIDS records. RMS officials stated that they considered BIDS records to be bank supervision records and that the RRS would be updated to reflect this 30-year retention period. However, based on the approved 5-year retention period, we determined that background investigation case records within BIDS dated back to January 2004 and approximately 13,800 records exceeded the retention period.[76]

[74] FDIC created these FOIA records between 2009 and 2010.
[75] The maximum retention period was 30 years.
[76] This number represents the amount of background investigation case records that exceeded 5 years as of December 31, 2018.

Office of Inspector General

Federal Deposit Insurance Corporation
Office of Inspector General
Office of Information Technology Audits and Cyber

Date: June 7, 2019

Memorandum To: Howard G. Whyte
Chief Information Officer and Chief Privacy Officer

Zachary N. Brown
Chief Information Security Officer

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

Subject **Advisory Memorandum** | *Unsecured Sensitive Information on the Network Shared Drives* | No. 2018-018

While conducting our ongoing audit of the FDIC's Privacy Program, we identified a security vulnerability warranting your urgent attention. As described below, we identified instances in which access to sensitive information, including sensitive Personally Identifiable Information (PII), stored on the FDIC's internal network was not properly secured. On May 23, 2019, we notified the Computer Security Incident Response Team (CSIRT) of this concern and the details of our observations. However, it is likely that additional sensitive information stored on the internal network is not properly secured.

Background

FDIC Circular 1360.9, *Protecting Sensitive Information*, states that it is the policy of the FDIC to safeguard sensitive information from unauthorized access. According to Circular 1360.9, only those individuals who have a legitimate need to access sensitive information in the performance of their duties shall be provided access. In addition, Federal information security policy and guidelines[1] require agencies to restrict access to sensitive information in accordance with the security principle of "least privilege." Least privilege refers to the practice of restricting user access to those information technology resources (including data) that are necessary to perform official duties.

The FDIC uses network shared drives to make information accessible to multiple users or groups of users over the FDIC's network. FDIC policy authorizes employees and contractor personnel to store business records, including records containing sensitive information, on network shared drives. According to information provided by the Division of Information Technology (DIT), the internal network contains over 200 resource servers capable of supporting shared drives. Each of these shared drives is capable of storing a significant number of documents. For example, we observed one network shared drive that contained over 35,000 folders. Each folder may contain multiple documents.

[1] Office of Management and Budget Circular Number A-130, *Managing Federal Information as a Strategic Resource*, published July 28, 2016 and National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013.

~~*Sensitive Information - For Official use Only*~~

Vulnerabilities Found

We reviewed a judgmental selection of six network shared drives and found multiple instances in which sensitive information, including sensitive PII, was not properly secured. According to DIT officials, [redacted] Sensitive information that was not properly secured included:

- Names, social security numbers, home addresses, and dates of birth of FDIC employees and failed bank customers;
- Names of employees who had been subject to disciplinary actions, such as letters of reprimand, suspensions, and terminations;
- Names of employees who had been placed on performance improvement plans or subject to wage garnishments; and
- Employee performance appraisals.

Conclusion

The lack of proper access control over sensitive PII increases the risk from insider threats[2] and the potential for breaches, which could lead to identity theft or other forms of consumer fraud against individuals. A breach of this information could also expose the FDIC to unnecessary costs and potential legal liability.

To reduce the risks described above, the Chief Information Officer (CIO) Organization should ensure that access to sensitive information, including sensitive PII, is properly restricted on all network shared drives. We request that you provide our Office with a written response describing the actions that the CIO Organization plans to undertake in order to address the risks described in this Memorandum, along with the timeframes for completing such actions. We request that your response be provided by June 21, 2019.

If you would like to discuss these concerns, please feel free to contact me at (703) 562-6316, or Laura Benton, IT Audit Manager, (703) 562-6320.

cc: Jennah Mathieson, CIO Organization
Arleas Upton Kea, Deputy to the Chairman and Chief Operating Officer
E. Marshall Gentry, Chief Risk Officer

[2] According to FDIC Circular 1600.7, *FDIC Insider Threat and Counterintelligence Program*, the term, "insider threat," refers to a threat posed to the FDIC or national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to a government resource. This threat may include unauthorized disclosure of unclassified sensitive information.

2

~~*Sensitive Information - For Official use Only*~~

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500

DATE: June 21, 2019

TO: Mark F. Mulholland, Assistant Inspector General
Information Technology Audits and Cyber

THROUGH: Howard G. Whyte /**Signed**/
Chief Information Officer and Chief Privacy Officer

FROM: Jennah Mathieson, Director /**Signed**/
Office of Chief Information Officer Management Services

Zachary N. Brown /**Signed**/
Chief Information Security Officer

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

SUBJECT: Management Response to the Advisory Memorandum Entitled
Unsecured Sensitive Information on the Network Shared Drives ~ No. 2018-018

Thank you for the opportunity to provide a written response to the Office of Inspector General's (OIG) Advisory Memorandum on the *Unsecured Sensitive Information on the Network Shared Drives,* issued June 7, 2019. In its memorandum, the OIG documented multiple instances in which sensitive information, including sensitive PII, was not properly secured. We have carefully considered and concur with the identified issues.

Our response provides a description of the actions the Chief Information Officer Organization (CIOO) plans to take to address the risks described in the OIG's memorandum including the timeframes for completing those actions. Our detailed response is organized by the areas of concern raised by the OIG and contains actions already completed, planned, or in process.

We appreciate your staff's time and effort and we expect that the actions taken in response to this advisory memorandum will further enhance the FDIC's access controls over sensitive information and reduce risk to the agency. Protecting sensitive information is critical to the FDIC's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system and continues to be a top priority at the FDIC.

MANAGEMENT RESPONSE

Advisory Area 1 – Lack of proper access controls over sensitive PII on network share drives

The FDIC uses network shared drives to make information accessible to multiple users or groups of users over the FDIC's network. FDIC policy authorizes employees and contractor personnel to store business records, including records containing sensitive information, on network shared drives. The Division of Information Technology (DIT), internal network contains over 200 resource servers capable of supporting shared drives. Each of these shared drives is capable of storing a significant number of documents. The OIG reviewed a judgmental selection of six network shared drives and found multiple instances in which sensitive information, including sensitive PII, was not properly secured. [redacted] Sensitive information that was not properly secured included names, social security numbers, home addresses, and dates of birth of FDIC employees and failed bank customers; employees who had been subject to disciplinary actions, such as letters of reprimand, suspensions, and terminations; and names of employees who had been placed on performance improvement plans or subject to wage garnishments.

Management Decision: (Concur)

Corrective Action:

We acknowledge that [redacted] However, there are file level permissions on the actual data hosted on the shares that should restrict access further to the appropriate user base. We further acknowledge that some instances where the file level permissions failed to prevent access exist and we are planning to address those instances as well as make improvements to ensure that further such instances are prevented and/or detected.

[redacted] is partnering with the Data Loss Prevention team from the OCISO to determine the location of all Sensitive information. Once we have the location of all of the sensitive information, we will determine the owner of the data, and we will work with them to lock down access to only those deemed appropriate by the data owner.

The Enterprise Data Governance Initiative (EDGI) will also work to develop a long term solution to better store the Corporations sensitive data.

2

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

The FDIC has a Data Loss Prevention (DLP) tool in place to monitor for egress of Sensitive data from the corporation today. The DLP tool will be used to scan our internal shared drives for Sensitive data on a regular basis.

In addition, the FDIC has in place a tool to monitor for open shares that includes alerting when new shares are created.

Estimated Completion Date:

The estimated completion date of the initial scans for sensitive information by the DLP and any associated remediation required as a result will be completed by December 31, 2019.

The estimated completion date for the development of a long term strategy will be done by December 31, 2019.

Any questions regarding this response should be directed to Jennah Mathieson at (703) 51[redacted] or [redacted] at (703) 51[redacted].

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Controls Branch
Russell G. Pittman, Director, DIT
Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch

3

FDIC

3501 Fairfax Drive, Arlington, VA 22226-3500 Chief Information Officer & Chief Privacy Officer

December 16, 2019

TO: Mark F. Mulholland
Assistant Inspector General for Audits

THROUGH: Arleas Upton Kea **/Signed/**
Deputy to the Chairman and Chief Operating Officer

Howard G. Whyte **/Signed/**
Chief Information Officer and Chief Privacy Officer

FROM: Jennah Mathieson **/Signed/**
Director
Office of Chief Information Officer Management Services

Zachary N. Brown **/Signed/**
Chief Information Security Officer

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

SUBJECT: Management Response to the Draft Audit Report Entitled *The FDIC's Privacy Program* (Assignment No. 2018-018)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on *The FDIC's Privacy Program* issued on November 14, 2019. The Chief Information Officer Organization fully supports the obligation of the FDIC to protect the privacy of individuals.

We are pleased that the OIG found that FDIC had generally implemented a privacy awareness and training program that identified privacy staffing and budgetary needs. Also, that the FDIC had established privacy competency requirements for crucial staff, and taken steps to ensure contractor compliance with privacy requirements.

In its report, the OIG also determined that the FDIC's controls and practices in four areas outlined in the report were partially adequate with all relevant privacy laws and OMB policy and guidance and made fourteen (14) recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and records management practices. FDIC management concurs with the report's findings and is committed to addressing each of the OIG's recommendations.

We appreciate your staff's time and effort, and we expect that FDIC actions already in progress and new activities we are taking in response to this draft report will further improve and help manage our risk posture. Responses to each recommendation are below:

MANAGEMENT RESPONSE

Recommendation 1 –

We recommend that the CIO/CPO:

1. Revise and implement policies, procedures, and/or guidance to address OMB policy and guidance for assessing privacy risk when categorizing information systems containing PII.

   Management Decision: Concur

   Corrective Action: The CIO/CPO has taken positive steps to ensure that privacy risk is appropriately assessed when categorizing systems containing Personally Identifiable Information (PII). FDIC's Privacy Threshold Analysis template was updated to ensure that the security impact levels determined using the categorization processes outlined in FIPS 199 are supplemented during the PTA adjudication process, when appropriate, with PII-specific enhancements. This new template was implemented in July 2019, and it is an integral component of our ongoing Privacy Continuous Monitoring program. A guide providing detailed information on how to complete the PTA is in process and will be issued during the first quarter of 2020.

   Estimated Completion Date: March 31, 2020

Recommendation 2 –

We recommend that the CIO/CPO:

2. Clarify and implement policies, procedures, and/or guidance that defines the role of the SAOP in reviewing and approving system categorizations for information systems containing PII.

   Management Decision: Concur

   Corrective Action: New or updated FDIC information systems are required to undergo a Privacy Threshold Analysis (PTA). The PTA template was updated to ensure that the security impact levels determined using the categorization processes outlined in FIPS 199 are supplemented during the PTA adjudication process, when appropriate, with PII-specific enhancements. The Authority to Operate (ATO) process has been updated to require Security Impact Analyses when a change to the system occurs, and requiring updated PTAs as necessary to reflect changes. These inputs are given consideration in conjunction with the execution of the ATO. All ATOs require CIO/SAOP review and approval.

   Estimated Completion Date: March 31, 2020

Recommendation 3 –

We recommend that the CIO/CPO:

3. Develop and approve privacy plans for all information systems containing PII consistent with OMB Circular A-130.

Management Decision: Concur

Corrective Action: The CIO/CPO ensures that privacy plans are developed and approved for information systems containing PII that are undergoing authorization or in the security control assessment process consistent with OMB Circular A-130. Further, we ensure that privacy plans are developed and approved for existing operational information systems in alignment with the continued execution of our Privacy Continuous Monitoring program. This process commenced in 2019 and is anticipated to be completed for all information systems containing PII over a three-year period, with priority for new and changing authorizations over the next year.

Estimated Completion Date: December 17, 2021

Recommendation 4 –

We recommend that the CIO/CPO:

4. Implement a PCM program to regularly assess the effectiveness of privacy controls.

Management Decision: Concur

Corrective Action: In April 2019, the CIO/CPO began execution of a Privacy Continuous Monitoring (PCM) program that aligns with the requirements set forth in OMB A-130 and ensures that privacy controls are regularly assessed for their effectiveness. Prior to that, FDIC devoted significant time, effort, and resources toward the rollout of the program, which included the development and issuance of a Privacy Program Plan, a Privacy Continuous Monitoring strategy, and the conduct of a PCM pilot. FDIC plans to continue the execution of the PCM program in accord with the PCM strategy. This process commenced in 2019 and is anticipated to be completed for all information systems containing PII over a three-year period, with priority for new and changing authorizations over the next year.

Estimated Completion Date: December 17, 2021

Recommendation 5 –

We recommend that the CIO/CPO coordinate with the Chief Operating Officer (COO) to:

5. Update policies and/or procedures to reflect the current organizational structure of the Privacy Program and responsibilities of agency personnel and component offices that support the FDIC's Privacy Program.

Management Decision: Concur

Corrective Action: The CIO/CPO will update the Privacy Program Plan and the Breach Response Plan to reflect the current organizational structure of the Privacy Program and the responsibilities of agency personnel currently supporting the FDIC's Privacy Program.

The OCISO Privacy section will work with DOA to identify those DOA policies and procedures that are relevant to the Privacy Program and assist the Division in updating them, as needed, to accurately reflect roles and responsibilities associated with supporting FDIC's Privacy Program.

Estimated Completion Date: July 30, 2021

Recommendation 6 –

We recommend that the CIO/CPO coordinate with the Chief Operating Officer (COO) to:

6. Establish a governance body or other governance mechanisms to assist the CRO with records management implementation and compliance.

Management Decision: Concur

Corrective Action: DOA Records and Information Management Unit (RIMU) will establish a Records and Information Management (RIM) working group to develop an enterprise approach to electronic and paper records management. DOA RIMU will update FDIC policies and procedures, including Directive 1210.1, to reflect agreed upon approaches, roles, and responsibilities.

Estimated Completion Date: June 1, 2020

Recommendation 7 –

We recommend that the CIO/CPO:

7. Complete and implement the data protection program policy directive, data labeling guide, and associated job aids.

Management Decision: Concur

Corrective Action: The Data Protection Program (DPP) Steering Committee approved a revised Document Labeling Framework and Implementation Plan approach in October 2019. The Data Protection Program will publish a labeling guide and user support materials, including job aids, by January 31, 2020, in support of initial Labeling Pilots and will develop and publish a Document Labeling Directive to formalize the labeling requirement for FDIC documents by September 30, 2020.

Estimated Completion Date: September 30, 2020

Recommendation 8 –

We recommend that the CIO/CPO:

8. Develop and implement controls to ensure that PII stored in network shared drives and in hard copy is regularly monitored and reviewed for compliance with privacy laws, regulations, policy, and guidelines.

Management Decision: Concur

Corrective Action: In September 2019, the CIOO performed scans of social security numbers (SSN) in network share files and used the results, in coordination with ISMs, to lock down access to only those deemed appropriate by the data owner.

The CIOO, in coordination with key stakeholders, is establishing a plan to monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic information. Additionally, the CIOO is establishing a plan, in coordination with relevant stakeholders, to monitor the security of hardcopy information in common areas via facility walkthroughs. This plan will be implemented in phases starting with facility walkthroughs of common office areas. Using existing communications channels, the CIOO will also remind Division and Office leadership of policy requirements for protecting sensitive electronic and hardcopy information by employees and contractors. Per the advisory memo dated June 21, 2019, the CIOO will work to develop a solution to better store the Corporation's sensitive data.

Estimated Completion Date: December 17, 2021

Recommendation 9 –

We recommend that the COO:

9. Ensure that Divisions and Offices complete File Plans.

Management Decision: Concur

Corrective Action: FDIC Directive 1210.1 currently requires that Records Liaisons (RL) and Division/Offices develop File Plans for approval by RIMU. While some of the Divisions/Offices have established File Plans, there are others that still need to complete those Plans. To ensure that all Divisions and Offices have an approved File Plan, DOA RIMU will elevate the issue for awareness and provide status of compliance at quarterly Operating Committee meetings to ensure that Division/Office leaders are aware of the requirement to develop File Plans for their sections. DOA RIMU will also provide additional training to RLs and stakeholders on using the Records Retention Schedule tool to create and update File Plans. DOA RIMU will work with the RLs to complete the remaining File Plans by the end of 2020.

Estimated Completion Date: December 31, 2020

Recommendation 10 –

We recommend that the COO:

10. Perform annual evaluations of the RIM program.

Management Decision: Concur

Corrective Action: DOA RIMU will conduct an evaluation of the FDIC RIM Program to ensure that Divisions/Offices are complying with Corporate policies and approved record retention schedules. An evaluation will be conducted annually.

Estimated Completion Date: December 31, 2020

Recommendation 11 –

We recommend that the CIO/CPO coordinate with the Deputy Director, Corporate Services Branch, DOA to:

11. Generate reports to monitor and audit compliance with the FDIC's records retention and disposition requirements.

Management Decision: Concur

Corrective Action: DOA RIMU will work with DIT to generate the necessary reports to monitor and audit compliance with the FDIC's records retention and disposition requirements.

Estimated Completion Date: December 31, 2020

Recommendation 12 –

We recommend that the Deputy Director, Corporate Services Branch, DOA, coordinate with the CIO/CPO to:

12. Finalize and implement a records management framework for FDIC information systems that ensures compliance with records retention requirements.

Management Decision: Concur

Corrective Action: DOA and CIO/CPO will develop a strategy to align a records information management (RIM) framework into current FDIC processes to evaluate the information created/captured, or maintained in FDIC systems. The end state are policies, governance, strategies, and evaluation mechanisms to provide a compliance framework that ensures records management capabilities are included in FDIC systems.

Estimated Completion Date: December 31, 2020

Recommendation 13 –

We recommend that the CIO/CPO:

13. Revise and implement processes to ensure that PIAs are completed and made available to the public prior to authorizing information systems containing PII to operate.

Management Decision: Concur

Corrective Action: In conjunction with the implementation and execution of FDIC's PCM Program, privacy staff have been appointed as members of SDLC-related governance committees. The committees are responsible for overseeing the introduction of new information systems to FDIC's IT environment, as well as the modification of information systems that are already a part of FDIC's IT environment. The Privacy Section's membership on these committees has improved the timeliness with which Privacy Section staff are made aware of new and modified information systems that may require privacy attention, such as the conduct of a PTA, PIA and privacy controls assessment. Additionally, privacy, in conjunction with the PCM program, will be integrated within the ATO process, thereby ensuring that privacy risks are assessed and addressed prior to information system authorizations

and re-authorizations. As the various facets of the PCM program continue to be executed, FDIC will have the ability to better ensure that PIAs are completed and made available to the public prior to authorizing information systems containing PII to operate.

Estimated Completion Date: December 31, 2020

Recommendation 14 –

We recommend that the CIO/CPO:

14. Revise and implement policy and/or processes to ensure PIAs are periodically reviewed, updated, and removed from the FDIC's public website when systems are retired.

Management Decision: Concur

Corrective Action: In April 2019, FDIC began execution of a PCM program that aligns with the requirements set forth in OMB Circular A-130, which ensures that PIAs are periodically reviewed and updated, as well as facilitates the removal of PIAs from the FDIC's public website when systems are retired. FDIC plans to continue the implementation and execution of the PCM program in accord with the PCM strategy.

Estimated Completion Date: December 31, 2020

If you have any questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk Governance and Policy, OCMS at 877-275-3342.

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Controls Branch
Greg S. Kempic, DOF, Risk Management and Internal Controls Branch

This table presents management's 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	The FDIC updated and implemented a new PTA template in July 2019 to ensure security impact levels determined using the categorization processes are supplemented during the PTA adjudication process, when appropriate, with PII-specific enhancements. The FDIC also plans to issue a guide on how to complete the PTA.	March 31, 2020	$0	Yes	Open
2	As stated above, the FDIC updated its PTA template and plans to issue a guide on how to complete the PTA. The FDIC also updated its Authority to Operate (ATO) process to require Security Impact Analyses and updated PTAs when system changes occur. Further, the CIO/SAOP reviews and approves all ATOs.	March 31, 2020	$0	Yes	Open
3	The FDIC began a process in 2019 to ensure privacy plans are developed and approved for all systems containing PII. The FDIC will fully implement this process over a 3-year period, with priority for new and changing authorizations over the next year.	December 17, 2021	$0	Yes	Open
4	In April 2019, the FDIC began executing a PCM program that aligns with OMB Circular A-130 and ensures privacy controls are regularly assessed for effectiveness. The FDIC plans to implement the PCM program for all information systems containing PII over a 3-year period, with priority for new and changing authorizations over the next year.	December 17, 2021	$0	Yes	Open
5	The FDIC will update the Privacy Program Plan and Breach Response Plan to reflect the current organizational structure of the Privacy Program and responsibilities of other Divisions and Offices supporting the Privacy Program. The FDIC will also identify and update, as needed, policies and procedures relevant to the Privacy Program to accurately reflect roles and responsibilities associated with supporting the Privacy Program.	July 30, 2021	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
6	The FDIC will establish a Records and Information Management working group to develop an enterprise approach for electronic and hardcopy records management. The FDIC will also update policies and procedures to reflect approved approaches, roles, and responsibilities.	June 1, 2020	$0	Yes	Open
7	In October 2019, the DPP Steering Committee approved a revised Document Labeling Framework and Implementation Plan. The DPP will publish a labeling guide and user support materials, followed by a Document Labeling Directive to formalize the labeling requirement for FDIC documents.	September 30, 2020	$0	Yes	Open
8	In September 2019, the FDIC scanned its network share files and used the results to restrict access to only those deemed appropriate by the data owner. The FDIC will establish a plan to monitor compliance with policy requirements for safeguarding sensitive electronic data, and a separate plan to monitor policy requirements for hardcopy information. In addition, the FDIC will remind Division and Office leadership of requirements for protecting sensitive electronic and hardcopy information. Further, the FDIC will develop a solution to better store its sensitive data.	December 17, 2021	$0	Yes	Open
9	The FDIC will provide quarterly updates to the FDIC Operating Committee regarding the status of Division and Office compliance with File Plan requirements. In addition, the FDIC will provide training to Record Liaisons and stakeholders on the use of the Records Retention Schedule tool to create and update File Plans. Further, DOA RIMU will work with Record Liaisons to complete remaining File Plans.	December 31, 2020	$0	Yes	Open
10	The FDIC will conduct annual evaluations of the FDIC's RIM Program for compliance with FDIC policies and approved record retention schedules.	December 31, 2020	$0	Yes	Open
11	DOA RIMU will work with DIT to generate the necessary reports to monitor and audit compliance with FDIC's records retention and disposition requirements.	December 31, 2020	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
12	The FDIC will develop a strategy to ensure records management capabilities are included in FDIC systems. This strategy will align a RIM framework with current processes for evaluating information created, captured, or maintained in FDIC systems. The FDIC plans to implement policies, governance, strategies, and evaluation mechanisms to ensure compliance.	December 31, 2020	$0	Yes	Open
13	The FDIC appointed Privacy Section staff to serve on governance committees related to the system development life cycle. Privacy Section staff are now made aware of new or updated information systems that may require privacy attention. In addition, the FDIC will integrate privacy into the ATO process to ensure privacy risks are assessed and addressed prior to information system authorizations.	December 31, 2020	$0	Yes	Open
14	In April 2019, the FDIC began executing a PCM Program that ensures PIAs are periodically reviewed an updated, and removed from the FDIC's public website when systems are retired. The FDIC plans to continue implementing its PCM program in accordance with its PCM strategy.	December 31, 2020	$0	Yes	Open

[a] Recommendations are resolved when —

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.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

☆☆☆☆☆☆

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.

FDIC OIG website	Twitter	OVERSIGHT.GOV ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE
www.fdicoig.gov	@FDIC_OIG	www.oversight.gov/