Office of Inspector General

Office of Information Technology Audits and Cyber
Report No. AUD-17-006

The FDIC's Processes for Responding to Breaches of Personally Identifiable Information

September 2017

Office of Inspector General

Executive Summary

The FDIC's Processes for Responding to Breaches of Personally Identifiable Information

Report No. AUD-17-006
September 2017

Why We Did The Audit

In fulfilling its mission of insuring deposits, supervising insured financial institutions, and resolving the failure of insured financial institutions, the FDIC collects and manages considerable amounts of personally identifiable information (PII). Such PII includes, for example, names, telephone numbers, home addresses, social security numbers, driver's license numbers, dates and places of birth, credit reports, education and employment histories, and the results of background checks. Implementing proper controls to safeguard this information and respond to breaches when they occur is critical to maintaining stability and public confidence in the nation's financial system and protecting consumers from financial harm.

We initiated this audit in response to concerns raised by the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs regarding a series of data breaches reported by the FDIC in late 2015 and early 2016. Many of these data breaches involved PII. The objective of the audit was to assess the adequacy of the FDIC's processes for (1) evaluating the risk of harm to individuals potentially affected by a breach involving PII and (2) notifying and providing services to those individuals, when appropriate. As part of our work, we judgmentally selected and reviewed the FDIC's handling of 18 of 54 suspected or confirmed breaches involving PII that the FDIC discovered during the period January 1, 2015 through December 1, 2016.

Background

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement agency-wide information security programs. According to the statute, agency information security programs must include procedures for detecting, reporting, and responding to security incidents, including breaches. FISMA requires agencies to notify affected individuals, pursuant to data breach notification policies and guidelines, as expeditiously as practicable and without unreasonable delay.

The FDIC's Chief Information Officer (CIO) serves as the Corporation's Chief Privacy Officer (CPO) and, as such, has overall responsibility for privacy issues. The FDIC's Chief Information Security Officer (CISO) serves as the principal advisor for the Corporation's information security and privacy programs. The CISO oversees the FDIC's Information Security and Privacy Staff (ISPS)—a group of security and privacy professionals within the CIO Organization who are responsible for investigating and remediating PII-related breaches.

The FDIC developed a Data Breach Handling Guide (DBHG), which was renamed the Breach Response Plan in April 2017, to govern its breach response activities. According to the DBHG, when a PII-related incident is discovered, it is referred to an Information Security Manager (ISM) within the affected FDIC division or office. The ISM serves as the focal point for investigating the incident and ensuring compliance with regulatory directives and policies. The ISM coordinates with a Privacy Staff member within ISPS who serves as the incident lead (ISPS Incident Lead).

The ISPS Incident Lead also determines whether to convene the Data Breach Management Team (DBMT)—a cross-divisional group of FDIC stakeholders responsible for addressing significant data

breaches or computer security incidents. The DBHG states that, in general, the FDIC aims to provide notification to affected individuals and/or entities within 10 business days of completing the analysis of breach data. Notifying potentially affected individuals as expeditiously as possible allows those individuals to take proactive steps quickly to protect themselves.

Audit Results

The FDIC established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate.

FDIC Did Not Complete Key Breach Investigation Activities and Notify Affected Individuals Timely. The FDIC did not complete key breach investigation activities (i.e., impact/risk assessments and/or convene the DBMT) within the timeframes established in the DBHG for 13 of 18 suspected or confirmed breaches that we reviewed. In addition, the FDIC did not notify potentially affected individuals in a timely manner for the incidents we reviewed. Specifically, it took an average of 288 days (more than 9 months) from the date the FDIC discovered the breaches to the date that the Corporation began to notify individuals. The breaches we reviewed potentially affected over 113,000 individuals. Breach investigations and notifications were not timely because the FDIC did not: have an Incident Response Coordinator to centrally manage its incidents; provide ISMs with adequate training; dedicate sufficient Privacy Staff to manage breach response activities; or take appropriate steps to ensure it was prepared to handle a large increase in required notifications. According to Office of Management and Budget (OMB) guidance, an agency's effective detection and expeditious response to a breach is important to reduce the risk of harm to potentially affected individuals and to keep the public's trust in the ability of the federal government to safeguard PII.

FDIC Did Not Adequately Document Key Assessments and Decisions. Our review of 18 suspected or confirmed breaches found that Incident Risk Analysis (IRA) forms did not clearly explain the rationale behind the overall impact/risk levels assigned to the incidents; some IRA forms were not substantially complete prior to convening the DBMT; the underlying analysis used to support assigned impact/risk levels for three breaches was inconsistent with the methodology in the DBHG; and the overall risk ratings recorded in the IRA forms for five breaches were not consistent with the risk mitigation actions taken by the FDIC. Not documenting the rationale for overall impact/risk ratings and decisions regarding notification and offering services to affected individuals limits the FDIC's ability to ensure consistency in the process. In addition, inaccurate and incomplete information in the IRA forms limited the ability of DBMT members to effectively evaluate the risk of harm to individuals and, therefore, delayed decision-making.

FDIC Needed to Strengthen Controls Over the DBMT. Although the DBHG describes the role and activities of the DBMT, the FDIC had not established a formal charter or similar mechanism for the DBMT that defines its purpose, scope, governance structure, and key operating procedures. Establishing charters is a common business practice at the FDIC and can help to ensure that roles, responsibilities, and expectations for stakeholders are clear. The FDIC had also not developed a process for briefing DBMT members on the outcome of their recommended actions. Such a process would allow DBMT members to more effectively leverage lessons-learned for future breach response decision-making and promote

consistency in the process. In addition, the FDIC did not provide DBMT members with specialized training to help ensure the successful implementation of their responsibilities.

FDIC Did Not Track and Report Key Breach Response Metrics. The DBHG identifies key categories of qualitative and quantitative metrics for benchmarking, tailoring, and continuously improving the FDIC's breach prevention and response capabilities. For example, the DBHG identifies reporting and response timelines as a key metric and establishes specific timeframes for completing key breach response activities. However, the FDIC generally did not track or report the metrics in the DBHG for the suspected or confirmed breaches we reviewed. Absent effective metrics, FDIC managers and other stakeholders lack timely, action-oriented information needed to assess program performance and ensure accountability.

Our report includes one additional matter that, although not within the scope of the audit, warranted management attention. Specifically, the FDIC needed to update its written CPO designation to reflect organizational changes that have occurred since the original designation was made in March 2005.

Recommendations and Corporation Comments

The FDIC has taken, or was working to take, a number of actions to strengthen its breach response processes. However, further control improvements are needed. Accordingly, our report contains seven recommendations addressed to the CIO/CPO that are intended to promote more timely breach response activities and strengthen controls for evaluating the risk of harm to individuals potentially affected by a breach and notifying and providing services to those individuals, when appropriate.

The FDIC provided a written response, dated September 25, 2017, to a draft of this report. In the response, FDIC management concurred with our recommendations and described planned and completed actions to address the recommendations. The FDIC expects to complete all corrective actions by September 30, 2018.

Contents

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

Office of Information Technology Audits and Cyber
Office of Inspector General

DATE: September 29, 2017

MEMORANDUM TO: Lawrence Gross, Jr.
Chief Information Officer and Chief Privacy Officer

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

SUBJECT: *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information*
(Report No. AUD-17-006)

In fulfilling its mission of insuring deposits, supervising insured financial institutions, and resolving the failure of insured financial institutions, the Federal Deposit Insurance Corporation (FDIC) collects and manages considerable amounts of personally identifiable information (PII).[1] Implementing proper controls to safeguard this information and respond to breaches when they occur is critically important to maintaining stability and public confidence in the nation's financial system and protecting consumers from financial harm.

We initiated this audit in response to concerns raised by the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs regarding a series of data breaches reported by the FDIC in late 2015 and early 2016. Many of these data breaches involved PII. The objective of this audit was to assess the adequacy of the FDIC's processes for (1) evaluating the risk of harm to individuals potentially affected by a breach involving PII and (2) notifying and providing services to those individuals, when appropriate.

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 a glossary of terms; Appendix 3 contains a list of acronyms and abbreviations; Appendix 4 contains the Corporation's comments; and Appendix 5 contains a summary of the Corporation's corrective actions.

[1] Certain terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Terms*.

Background

According to the United States Computer Emergency Readiness Team (US-CERT),[2] federal government agencies reported more than 50,000 security incidents involving PII to US-CERT from 2014 through 2016. These incidents underscore the importance of having an effective response capability in place that includes procedures for assessing the risk of harm to potentially affected individuals and notifying those individuals of the harm they may experience when a breach of their personal information occurs.

On January 3, 2017, the Office of Management and Budget (OMB) issued its Memorandum M-17-12, entitled *Preparing for and Responding to a Breach of Personally Identifiable Information*.[3] OMB Memorandum M-17-12 describes the gravity of PII breaches and the importance of handling these issues appropriately and seriously. Specifically, the memorandum states:

> "Over the past decade, discussions about the risk of harm to individuals resulting from a breach have generally focused on financial-or credit-related identity theft, such as using a stolen credit card number, opening a new bank account, or applying for credit in another person's name. Today, however, malicious actors use stolen PII, modern technology, and forged identity documents to:
>
> - seek employment;
> - travel across international borders;
> - obtain prescription drugs;
> - receive medical treatment;
> - claim benefits;

What is a Breach?

OMB defines the term breach as a type of security incident that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. A breach can be inadvertent, such as a loss of hard copy documents or portable electronic storage media, or deliberate, such as a successful cyber-based attack by a hacker, criminal, or other adversary.

[2] US-CERT is an organization within the Department of Homeland Security that assists federal civilian agencies with their incident handling efforts. The Federal Information Security Modernization Act of 2014 (FISMA 2014) requires federal agencies to report security incidents to US-CERT, which analyzes the information to identify trends and indicators of attack across the federal government.

[3] OMB Memorandum M-17-12 had not been issued at the time the FDIC discovered and began investigating the suspected or confirmed breaches covered by this audit. Accordingly, we did not assess the FDIC's processes for compliance with OMB Memorandum M-17-12. We did, however, consider this guidance and relevant updates to the FDIC's policies, procedures, and guidelines as context in formulating our conclusions and recommendations.

- file false tax returns; and

- aid in other criminal activities.

> Additionally, identity theft – the harm most often associated with a breach – remains a significant problem in the United States. Identity theft represented 16 percent (or 490,220) of the over 3 million complaints received by the Federal Trade Commission (FTC) in 2015. In 2014, the Department of Justice reported that 17.6 million individuals, or 7 percent of all U.S. residents age 16 or older, were victims of one or more occurrences of identity theft. Moreover, new types of identity theft are emerging, such as synthetic identity theft, which occurs when a malicious actor constructs a new identity using a composite of multiple individuals' legitimate information along with fabricated information.
>
> As the ways in which criminals can exploit PII have evolved, so too have the ensuing types of harm to potentially affected individuals. Identity theft can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and, in rare cases, risk to personal safety." [Footnotes excluded.]

As a federal deposit insurer and the primary federal regulator of state-chartered, nonmember financial institutions, the FDIC collects and maintains a significant quantity of PII on customers of insured institutions. Further, as an employer, an acquirer of services, and receiver for failed institutions, the FDIC collects and maintains PII pertaining to its employees, contractors, and the customers of failed institutions. Such PII includes names, home addresses, telephone numbers, social security numbers (SSN), driver's license/state identification numbers, Employee Identification Numbers (EIN), and dates and places of birth. It also includes, but is not limited to, information related to education, finances (e.g., bank account numbers, access or security codes, credit reports, and personal identification numbers), medical histories, criminal histories, and employment histories.

A breach of PII could expose the FDIC to unanticipated costs, potential legal liability, and negative publicity that could erode the public's trust in the Corporation. In 2015, for example, the Office of Personnel Management (OPM) discovered a cyber-intrusion into its systems that exposed the personal information of more than 21 million individuals. In response to this incident, OPM, in conjunction with other federal agencies, awarded a contract for data breach recovery services to affected individuals valued at approximately $330 million.

That same year, the Government Accountability Office (GAO) added the protection of PII to its government-wide High Risk List.[4] In doing so, GAO noted that the risk of PII exposure and compromise have increased, due to advancements in technology, an increased

[4] Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation. These agencies and program areas are reflected on GAO's High Risk List.

sophistication of hackers and others with malicious intent, and the extent to which federal agencies and private companies collect sensitive information about individuals.

Federal Laws, Policies, and Guidelines

A number of federal statutes and government-wide policies and guidelines have been established to assist federal agencies in developing and implementing effective breach response capabilities. Congress has also enacted a number of statutes requiring federal agencies to assign overall responsibility for privacy protection and compliance to a senior agency official. Laws, policies, and guidelines that are particularly relevant to the scope of our audit are described below.[5]

The Federal Information Security Management Act (FISMA) and Its Amendments. Enacted in 2002, FISMA required federal agencies to develop, document, and implement agency-wide information security programs to provide security for their information and information systems and to support the operations and assets of the agencies, including information and information systems that are provided or managed by another agency, contractor, or other source. In 2014, the FISMA statute was amended and updated. Among other requirements, FISMA 2014 places additional requirements upon federal agencies to develop procedures for detecting, reporting, and responding to security incidents, including breaches. Such procedures are to be consistent with federal standards and guidelines and include steps for mitigating risks before substantial damage occurs.

The FISMA 2014 statute also requires agencies to develop procedures for notifying affected individuals pursuant to data breach notification policies and guidelines established by OMB. According to the statute, agencies must notify affected individuals "as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access."[6]

Section 522 of Division H of the Consolidated Appropriations Act, 2005, as amended (Section 522). Enacted in December 2004, Section 522 requires federal agencies to have a Chief Privacy Officer (CPO) "to assume primary responsibility for privacy and data protection policy." The statute assigns a number of responsibilities to the CPO, including:

1) Assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form;

2) Assuring that the technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy

[5] Appendix 1 contains a complete list of the laws, policies, and guidelines that we considered when planning and conducting our work.
[6] Public Law 113-283, §3558 (d)(1), 128 Stat. 3073, 3085 (2014).

policies and practices governing the collection, use, and distribution of information in the operation of the program;

3) Training and educating employees on privacy and data protection policies to promote awareness of, and compliance with, established privacy and data protection policies; and

4) Ensuring compliance with privacy and data protection policies.

It should be noted that not all of these statutory responsibilities relate to information technology or computer systems. Many responsibilities focus on the privacy of individuals, which would include, for example, FDIC programs, policies, and procedures that affect its personnel, as well as those that impact bank customers.

Guidance Issued by OMB. On May 22, 2007, OMB issued Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. OMB Memorandum M-07-16 required federal agencies to develop and implement breach response policies and procedures and a plan that addressed, among other things, processes for: assessing the likely risk of harm and level of risk in order to determine whether notification to affected individuals is required; determining who should be notified; providing notification without unreasonable delay; and ensuring that notifications include appropriate content. OMB Memorandum M-07-16 was in effect when the activities covered by this audit took place.

On February 9, 2016, the President issued Executive Order 13719, entitled *Establishment of the Federal Privacy Council*. This Order required that OMB issue a revised policy on the role and designation of the Senior Agency Officials for Privacy (SAOPs). The Order further stated that OMB should provide guidance regarding the SAOP's required level of expertise, adequate level of resources, and other matters.

On September 15, 2016, OMB issued Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy,* which addressed the roles and responsibilities of the SAOP, as required by Executive Order 13719. OMB Memorandum M-16-24 states, in part: "[e]ach agency shall develop, implement, document, maintain, and oversee an agency-wide privacy program . . . led by an SAOP who is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission." Further, "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. 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 . . . ." OMB Memorandum M-16-24 also states that the SAOP "shall manage privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems."

On January 3, 2017, OMB issued follow-up guidance in its Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. This Memorandum M-17-12 rescinded the earlier OMB guidance Memorandum M-07-16 and reflected changes in laws, policies, and best practices that emerged after OMB first required agencies to develop plans for responding to breaches.[7] OMB Memorandum M-17-12 sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. OMB Memorandum M-17-12 contains detailed guidance on numerous topics, including the following:

- **Assessing the Risk of Harm to Individuals Potentially Affected by a Breach**. OMB Memorandum M-17-12 includes factors the agency shall consider when assessing the risk of harm to potentially affected individuals. These factors include the Nature and Sensitivity of PII (e.g., the data elements, context, private information, vulnerable populations, and permanence); Likelihood of Access and Use of PII (e.g., the security safeguards, format and media, duration of exposure, and evidence of misuse); and Type of Breach (e.g., the intent and recipient). According to OMB Memorandum M-17-12, "In many circumstances, the SAOP may be unable to determine whether a breach was intentional or unintentional. In these instances, the SAOP shall consider the possibility that the breach was intentional."

- **Notifying Individuals Potentially Affected by a Breach**. "The SAOP, in coordination with the breach response team when applicable, shall consider the . . . Timeliness of the Notification, including the requirement to provide notification as expeditiously as practicable, without unreasonable delay."

- **Tracking and Documenting the Response to a Breach**. "The process for internally tracking each reported breach shall allow the agency to track and monitor the following: The total number of breaches reported over a given period of time; the status for each reported breach, including whether the agency's response to a breach is ongoing or has concluded; the number of individuals potentially affected by each reported breach; the types of information potentially compromised by each reported breach [parenthetical reference omitted]; whether the agency, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach; whether the agency, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach; and whether a breach was reported to US-CERT and/or Congress."

[7] Such changes include FISMA 2014 and recommendations in OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, issued in October 2015. In issuing Memorandum M-17-12, OMB rescinded and replaced its previously-issued guidance (including Memorandum M-07-16) intended to help agencies safeguard their PII holdings and take appropriate steps when they lose control of such information.

Guidance Issued by the National Institute of Standards and Technology (NIST). NIST Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*, Revision 2, dated August 2012, provides guidance for establishing computer security incident response capabilities and handling incidents efficiently and effectively. Among other things, NIST SP 800-61 recommends that organizations:

- Establish an incident response policy and a plan that provides a roadmap for implementing the incident response capability;
- Designate a single employee, with one or more alternates, to be in charge of incident response;
- Select an appropriate team structure and staffing model for handling incidents;
- Select personnel with the appropriate skills for addressing incident response;
- Provide training to incident response team members; and
- Establish metrics to measure performance and effectiveness.

With respect to notifications to potentially affected individuals, NIST SP 800-61 refers to both OMB guidance and breach notification laws enacted by states.

Roles and Responsibilities

In February 2005, OMB issued its guidance Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, which requested that federal agencies designate an SAOP with overall responsibility for information privacy issues. On March 9, 2005, the FDIC Chairman designated the Chief Information Officer (CIO) and Director, Division of Information Technology (DIT), to serve as CPO of the FDIC, with overall agency-wide responsibility for information privacy issues. The CIO/CPO also serves as the FDIC's SAOP.

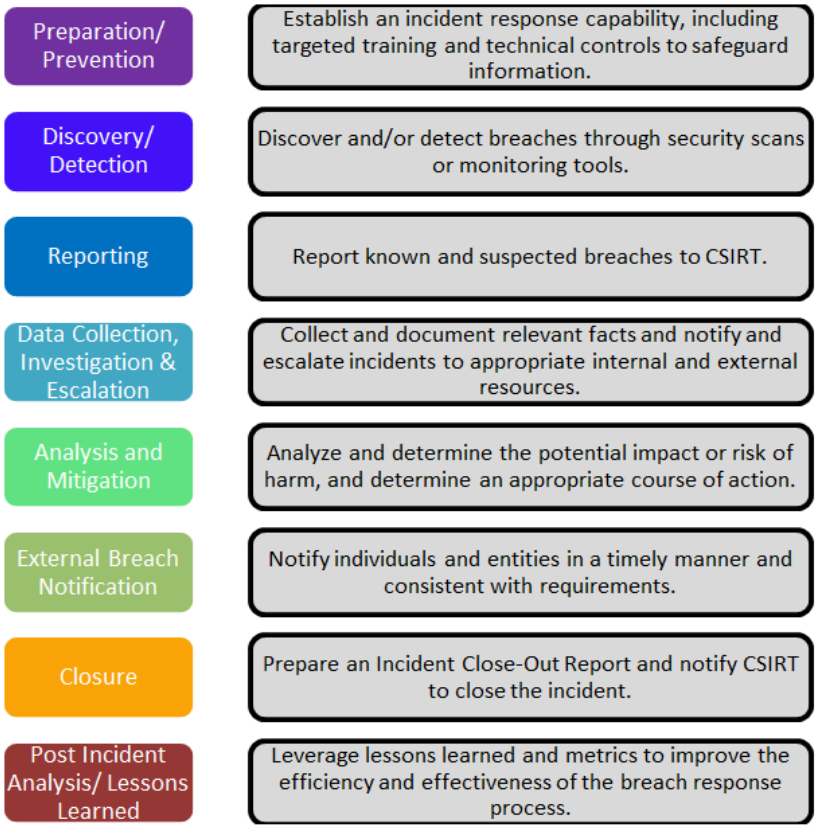
According to the FDIC's Data Breach Handling Guide (DBHG),[8] the FDIC's Chief Information Security Officer (CISO) serves as the principal advisor for the Corporation's IT security and privacy programs. The CISO reports to the CIO/CPO, who reports to the FDIC Chairman. According to the FDIC's DBHG, the CISO oversees the FDIC's Information Security and Privacy Staff (ISPS)—a group of security and privacy professionals within the Chief Information Officer Organization (CIOO) who are responsible for investigating and remediating breaches. The FDIC has also designated a Privacy Program Manager within ISPS to enhance and implement a comprehensive privacy program.

[8] On April 7, 2017, the FDIC replaced its DBHG with the Breach Response Plan (BRP).

The FDIC's Breach Response Processes

FDIC Circular 1360.9, *Protecting Sensitive Information*, states that if PII is suspected or known to be lost or otherwise compromised, immediate notification must be made to the FDIC Help Desk/Computer Security Incident Response Team (CSIRT), the appropriate FDIC supervisor or Contract Oversight Manager, and division or office Information Security Manager (ISM) at the earliest available opportunity. The Circular states that the DBHG must be followed for any loss, misuse, or unauthorized access of PII in order to reduce the potential harm or embarrassment to individuals and the Corporation.

Figure 1: Stages of the Breach Response Lifecycle



Source: The DBHG, Versions 1.4 dated April 16, 2015 and 1.5 dated June 6, 2016 (the versions in effect for the period covered by the audit).

The DBHG breaks the process of responding to a breach into eight stages (see Figure 1). Our audit focused on the FDIC's breach response activities within three of these stages: *Data Collection, Investigation, and Escalation; Analysis and Mitigation*; and *External Breach Notification*. A description of the roles, responsibilities, and activities during these three stages follows.

Data Collection, Investigation, and Escalation

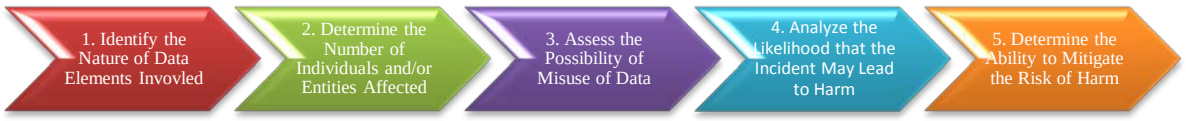
According to the DBHG, when CSIRT is notified of a PII-related incident, CSIRT is responsible for gathering and documenting pertinent information about the incident and forwarding the materials to the appropriate FDIC managers, the division or office ISM, and a Privacy Staff member within ISPS who serves as the incident lead (ISPS Incident Lead). CSIRT must also notify US-CERT about the incident within 1 hour of discovery. Upon

notification, the ISM serves as the point of contact to investigate, assess, and ensure compliance with all regulatory directives and policies.

Analysis and Mitigation

According to the DBHG, the ISM coordinates with the ISPS Incident Lead to begin preparing an Incident Risk Analysis (IRA) form. The IRA form includes (among other things) an impact/risk assessment that considers five factors (as depicted in Figure 2): (1) the nature of the data; (2) the number of individuals or entities affected; (3) the possibility of misuse; (4) the likelihood that the incident may lead to harm for individuals or entities; and (5) the ability of the FDIC to mitigate the risk of harm. The DBHG states that this analysis shall be followed when assessing the likely risk of harm caused by a breach and determining an appropriate course of action. The methodology is based on OMB guidance and NIST risk assessment guidelines.

Figure 2: The Five-Factor Incident Risk Analysis Methodology



Source: The DBHG, Versions 1.4 dated April 16, 2015 and 1.5 dated June 6, 2016 (the versions in effect for the period covered by the audit).

For each of the five factors, the ISM, in coordination with the ISPS Incident Lead, must respond to a series of questions (see Figure 3). The answers to these questions are used to determine an impact rating of High, Moderate, or Low for each factor that reflects the potential harm that could result if PII were inappropriately accessed, used, or disclosed. These ratings are recorded in the IRA form.

Based on this analysis, the FDIC assigns an overall impact/risk level of High, Moderate, or Low to the breach. The FDIC uses this overall rating to determine an appropriate course of action, such as notifying potentially affected individuals and/or offering them services, to mitigate the risk of the breach. The DBHG states that the ISPS Incident Lead and ISM should generally complete the impact/risk assessment within 1 to 3 business days of receiving notification from CSIRT that a potential breach has occurred.

Figure 3: Risk Factors and Associated Questions

Nature of the Data	Number of Individuals or Entities Affected	Possibility of Misuse	Likelihood Incident May Lead to Harm	Ability of the FDIC to Mitigate Harm
•What type of data is involved? •Does the context of use affect the overall sensitivity of the data?	•What is the number of potentially affected individuals and/or entities?	•Was the data protected or secured? •Is there evidence or indication that unauthorized individuals or entities actually accessed, downloaded, or viewed the data? •Is it likely that the individual(s) who gained access to the data will know the value of the data and use it for unauthorized purposes or sell it to others?	•Was the incident the result of theft or another criminal act? •Is there evidence or indication that the data was deliberately targeted or intentionally provided to unauthorized parties? •Is there evidence that the compromised information is being used to commit identity theft or other harm?	•During the investigation, was it discovered that the information was accessed, viewed, disclosed, or distributed to unauthorized parties? •Can the data be used to open new accounts or commit identity theft? •Can the data be used to cause embarassment or other harm?

Source: The FDIC's IRA Form Template.

The DBHG states that the decision to provide notification should give greater weight to Factor 3 (*Possibility of Misuse of Data*) and Factor 4 (*Likelihood the Incident May Lead to Harm*).

At the conclusion of the impact/risk assessment, the ISPS Incident Lead determines whether to convene the Data Breach Management Team (DBMT)—a cross-divisional group of FDIC stakeholders that is responsible for addressing "significant" data breaches or computer security incidents. A "significant" data breach is one that: (1) potentially impacts 100 or more individuals and/or entities; (2) involves circumstances that are unusual or that may result in significant reputational damage, cost, or media attention; or (3) involves the loss or compromise of critical sensitive information which may significantly affect the FDIC's mission or operations. The DBHG states that the ISPS Incident Lead will convene the DBMT, if applicable, within 24 hours of completing the impact/risk assessment. Members of the DBMT consist of the following:

- CIO/CPO, and/or designee, who chairs the DBMT;
- CISO, and/or designated information technology (IT) security specialists;
- Privacy Program Manager, and/or designated privacy specialists;

- ISPS Incident Lead;
- Legal Division, Deputy General Counsel, and/or designee;
- Office of Communications Director, and/or designee;
- Chief Risk Officer, and/or designee;
- Affected division or office director, and/or designee;
- ISM/Divisional Incident Response point(s) of contact (POC) from the affected division or office; and
- Appropriate FDIC program area specialists, such as specialists from the Office of Legislative Affairs, Office of Inspector General (OIG), and Internal/External Ombudsman.

According to the DBHG, the DBMT reviews and verifies the impact/risk assessment in terms of the level of harm posed to affected individuals/entities, the financial sector (if applicable), and the Corporation; makes a recommendation to the CIO/CPO as to whether the incident constitutes a breach; and determines and manages an appropriate course of action to respond to the breach and mitigate any harm. Breaches that are not considered significant are assessed and managed to closure by the ISPS Incident Lead. The affected division or office and ISPS Incident Lead may consult with the DBMT in developing a course of action for non-significant incidents, as needed.

External Breach Notifications

According to the DBHG, the FDIC may determine that it is appropriate to notify potentially affected individuals and entities. If convened, the DBMT recommends to the CIO/CPO (or designee) appropriate external breach communications and notifications, including notifications to individuals, financial institutions, or other entities. The DBHG also provides guidance regarding the content, timing, method, and recipients of the notifications.

The DBHG states that, in general, the FDIC aims to provide notification to affected individuals and/or entities within 10 days of completing the analysis of breach data. Notifying potentially affected individuals as expeditiously as possible allows those individuals to take proactive steps quickly to protect themselves. Such steps depend on the nature and circumstances of the breach but may include such things as more vigilant monitoring of credit reports for suspicious or unusual activity; obtaining credit monitoring services; requesting that the major credit reporting bureaus place a “fraud alert” on the individual’s credit report to notify creditors that new credit should not be issued without the individual’s permission; and reviewing publicly available resources, such as those offered by the FTC.

If notifications to individuals are recommended, the DBMT determines whether to recommend additional mitigating strategies, such as credit monitoring and/or identity theft insurance services, for potentially affected individuals. Depending on the circumstances of the incident, the FDIC CIO/CPO, in coordination with the Executive Office, may decide that it is appropriate to notify individuals of a breach without providing credit monitoring services. According to OMB Memorandum M-17-12, choosing not to provide services is a decision separate from the decision to provide notification, and there may be circumstances where potentially affected individuals are notified but not provided services. Regardless of these decisions, a fundamental tenet of the DBHG is that an effective and quick response is critical to the success of the FDIC's efforts to prevent or minimize harm to individuals caused by a breach.

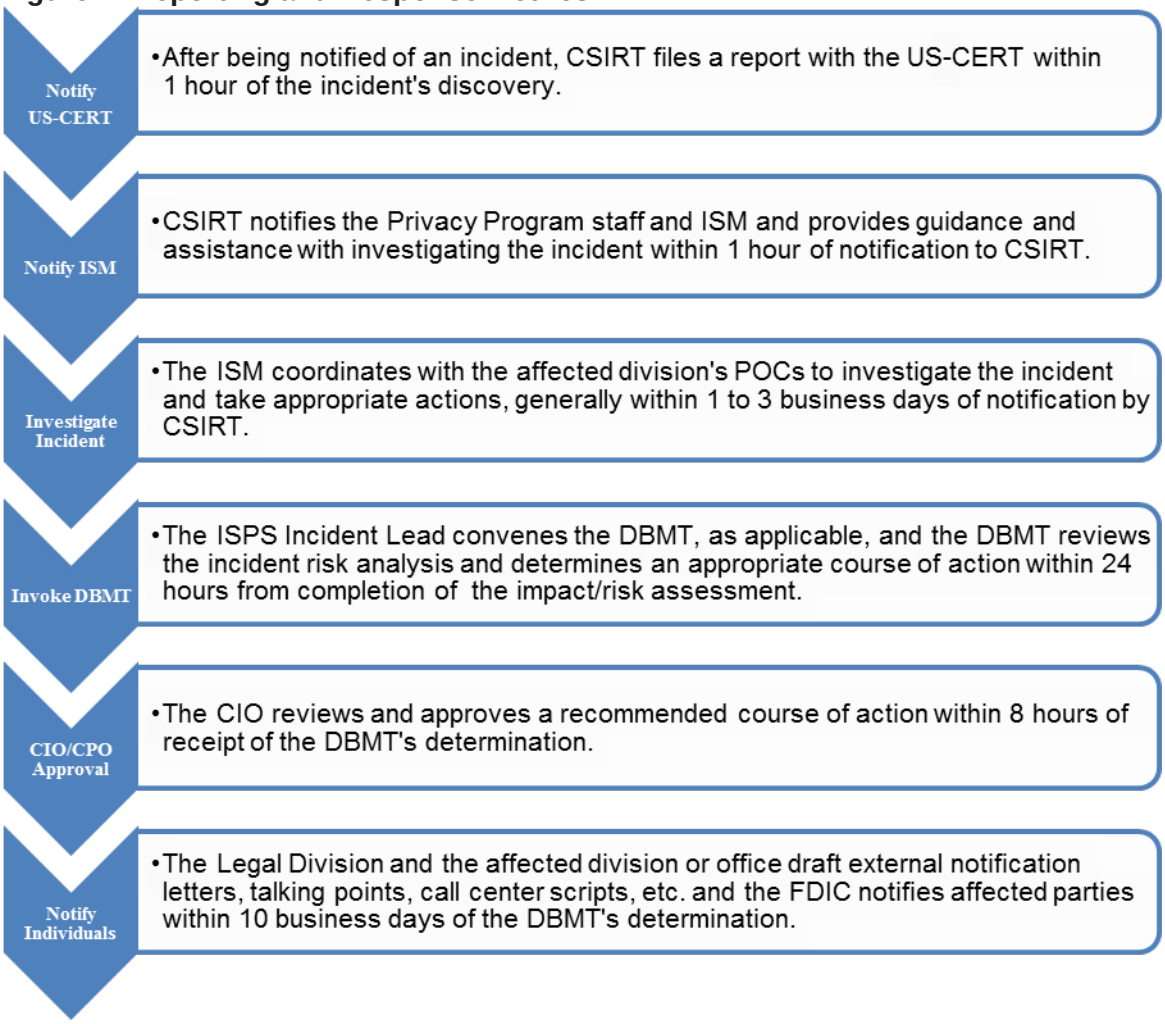
Performance Metrics

NIST SP 800-61, *Computer Security Incident Handling Guide*, Revision 2, states that organizations should have an incident response plan that includes, among other things, metrics for measuring and evaluating the effectiveness of incident response.[9] Metrics can be useful for identifying trends and systemic weaknesses, analyzing the adequacy of control activities, and monitoring the accomplishment of goals and objectives.

The DBHG states that metrics provide a frame-of-reference for gauging and benchmarking the overall efficiency and effectiveness of the FDIC's breach prevention and response capabilities, while driving operational improvement and enhancing data safeguards. The DBHG identifies key categories of metrics that the FDIC uses to benchmark, tailor, and continuously improve its breach prevention and response capabilities. These include, for example, timeframes for performing certain breach investigation activities, invoking the DBMT, and providing notification to potentially affected individuals. Figure 4 describes key reporting and response metrics.

[9] NIST SP 800-61 includes examples of potentially useful metrics, such as the total amount of labor (i.e., cost) spent working on an incident and the elapsed time from the beginning of the incident to each stage of the incident handling process.

Figure 4: Reporting and Response Metrics



Source: The DBHG, Versions 1.4 dated April 16, 2015 and 1.5 dated June 6, 2016 (the versions in effect for the period covered by the audit).

Audit Results

The FDIC established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate. Specifically, we found that the FDIC did not:

- Meet internally-established timeframes for completing key breach investigation activities or provide timely notifications to potentially affected individuals for the breaches we reviewed;

- Clearly explain in IRA forms its rationale behind the overall impact/risk levels (i.e., High, Moderate, or Low) assigned to breaches or ensure that IRA forms contained accurate and complete information;

- Establish a charter or similar governance mechanism for the DBMT, develop a process for briefing DBMT members on the outcomes of investigations and actions taken to address DBMT recommendations to resolve breaches, or provide specialized training for DBMT members; or

- Use performance metrics to measure and assess the effectiveness of key breach response processes.

The FDIC did not have sufficient resources in place to address the dramatic increase in breach investigation activities and notifications to affected individuals in 2016. In addition, according to FDIC internal assessments, those charged with investigating PII-related breaches did not always have the necessary skills and training to ensure the successful performance of their duties. The weaknesses described in this report can increase the risk of harm to individuals affected by a breach, expose the FDIC to increased risk, and impair the Corporation's ability to comply with statutory and federal policy requirements, such as FISMA 2014 that requires agencies to notify potentially affected individuals as expeditiously as practicable and without unreasonable delay. As described in this report, while the FDIC took a number of steps to strengthen its breach response processes, it needed to implement further control improvements.

Our report also includes an other matter that, although not within the scope of the audit, warrants management attention. Specifically, the FDIC needed to update its written CPO designation to reflect organizational changes that have occurred since the original designation was made in March 2005.

FDIC Did Not Complete Key Breach Investigation Activities and Notify Affected Individuals Timely

We reviewed 18 of 54 suspected or confirmed breaches involving PII that the FDIC discovered during the period January 1, 2015 through December 1, 2016 to assess the timeliness of key breach investigation activities and notifications to potentially affected individuals.[10] Six of the 18 breaches we reviewed were designated by the FDIC as "major incidents" as that term was defined in OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated

[10] See Appendix 1 for a detailed description of our sampling methodology.

October 30, 2015.[11] Although FISMA and OMB guidance emphasize the importance of notifying potentially affected individuals as expeditiously as practicable,[12] the statute and guidance do not specify timeframes for completing investigations and making notifications. Accordingly, we used the timeframes in the DBHG to assess the timeliness of the FDIC's efforts to complete key breach investigation and notification activities.

In summary, we found that the FDIC did not complete key breach investigation activities (i.e., impact/risk assessments and/or convening the DBMT) within the timeframes established in the DBHG for 13 of the 18 suspected or confirmed breaches that we reviewed. In addition, of the 18 incidents we reviewed, the FDIC notified individuals in 5 cases. For each of these five cases, the FDIC did not notify affected individuals in a timely manner. Figure 5 illustrates the time it took the FDIC to investigate and notify individuals for the five breaches that involved notifications. Notably, it took an average of 288 days (more than 9 months) from the date that the FDIC discovered the breaches to the date that the Corporation began to notify individuals that their personal information was involved in a breach.[13]

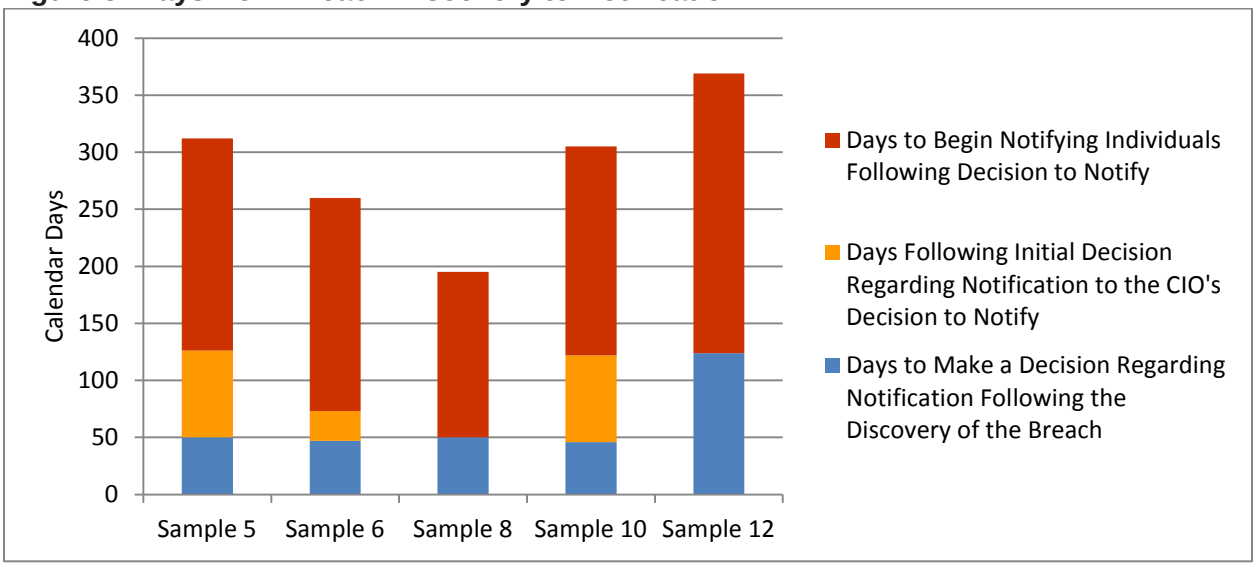
According to OMB Memorandum M-17-12, an agency's effective detection and expeditious response to a breach is important to reduce the risk of harm to potentially affected individuals and to keep the public's trust in the ability of the federal government to safeguard PII. Consequently, the longer it takes to complete breach investigation activities and notify potentially affected individuals, the greater the risk of harm that may come to individuals because they cannot quickly take proactive actions to protect themselves.

[11] OMB subsequently revised the definition of major incident in Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, dated November 4, 2016. The FDIC determined that 5 of the 6 major incidents we reviewed warranted notification to affected individuals.

[12] We also noted that Title 12, Code of Federal Regulations, Supplement A to Appendix B to Part 364, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, states that if a financial institution "determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible."

[13] According to ISPS records, the FDIC mailed notification letters to 107,126 (or 94 percent) of the 113,601 potentially affected individuals on the first day that it began to notify individuals of the incidents. The FDIC mailed notification letters to the remaining potentially affected individuals between 10 days and 4 months after the initial mailings. ISPS officials informed us that the FDIC had difficulty obtaining accurate addresses for these remaining individuals, which added to the amount of time needed to notify them.

Figure 5: Days from Breach Discovery to Notification



Source: OIG analysis of FDIC breach documentation.

With respect to Sample Items 5 and 10 in Figure 5, the DBMT determined on February 26, 2016 that notification to potentially affected individuals was not warranted. For Sample Item 6, the DBMT determined on April 13, 2016 that notification to potentially affected individuals was not warranted. Subsequent to these decisions, on May 12, 2016, the CIO/CPO directed ISPS to begin notifying individuals that their personal information was involved in a breach. The CIO/CPO informed us that this change occurred because there was a disconnect between the DBMT's earlier decision not to notify individuals and the fact that the FDIC had subsequently reassessed the incidents and determined that they were major as a result of our prior audit work.[14] The CIO/CPO added that the FDIC wanted to address any potential public concern that the Corporation was not notifying individuals who were potentially impacted by a major incident. The FDIC Chairman also informed us that the decision to notify and offer credit monitoring services for individuals potentially affected by Sample Items 5, 6, and 10 was in response to Congressional concerns raised during a May 12, 2016 hearing.[15]

For Sample Item 12, the DBMT had not yet made a determination about whether to notify potentially affected individuals when the FDIC decided to make notifications on May 12, 2016. For Sample Item 8, the DBMT determined on August 5, 2016 that individuals should be notified.

We reviewed selected notification letters sent to potentially affected individuals for the breaches identified in Figure 5 and found that they contained the type of information

[14] See OIG report, entitled *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*, (Report No. AUD-16-004, dated July 2016 and updated February 2017).
[15] Committee on Science, Space, and Technology, Subcommittee on Oversight, U.S. House of Representatives hearing, entitled "FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?" held on May 12, 2016.

recommended in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. Such information included a description of the breach; the actions the FDIC was taking to investigate the breach; the steps that individuals could take to protect themselves; and contact information should the individuals have questions.

Breach Investigative Activities

The DBHG states that the ISPS Incident Lead and ISM should generally complete the investigative activities described in the *Data Collection, Investigation, and Escalation* and *Analysis and Mitigation* stages of the breach life cycle within 1 to 3 business days of receiving notification from CSIRT that a potential breach has occurred. Such investigative activities include assessing the risk of harm to potentially affected individuals and recording the results of that assessment in the IRA form. The DBHG recognizes that the facts and circumstances of each incident are situational and that some investigations may require additional time to complete. In such situations, the ISPS Incident Lead may extend the timeframes defined in the DBHG. The DBHG is silent on whether this extension should be documented and whether it requires a higher level of approval. However, the DBHG states that the goal is to assess the risk and potential impact of the incident and determine a recommended course of action within 48 hours of reviewing and assessing the notification from CSIRT.

Based on our analysis of the IRA forms and other investigative records,[16] we determined that key investigative activities were not completed within the 1 to 3 day timeframe for at least 12 (or 67 percent) of the 18 incidents we reviewed. Our analysis indicates that investigative activities for these 12 incidents took between 7 and 32 business days to complete, representing an average of 21 days. In many cases, the FDIC did not complete investigative activities within the 1 to 3 day timeframe because ISMs had to await the retrieval of removable media that were involved in the breaches, conduct considerable data analysis and research, and coordinate with various FDIC divisions and offices. We found no documentation, however, that the ISPS Incident Leads for these incidents extended the timeframes for completing investigative activities. Absent revised timeframes, the FDIC cannot effectively measure the timeliness of its breach investigation activities.

The DBHG also states that the ISPS Incident Lead will convene the DBMT, if applicable, within 24 hours of completing the impact/risk assessment. Based on our analysis of IRA forms and other investigative records, we determined that the DBMT was not invoked within 24 hours of completing this assessment for at least 8 of 11 breaches we reviewed where the DBMT was convened. Our analysis indicates that for these eight breaches, it took

[16] ISMs did not document when breach investigations began and ended. In the absence of this information, we analyzed the IRA forms and other investigative records to determine approximately when investigations began and ended.

between 3 and 29 calendar days (an average of 14 calendar days) to convene the DBMT after the ISM's assessment was completed.

Breach Notification Decisions and Notifications to Affected Individuals

The DBHG states that, in general, the FDIC aims to provide notification to affected individuals and/or entities within 10 business days of completing the analysis of breach data. We reviewed five suspected or confirmed breaches that involved notifications to individuals. Of these five breaches, none were made within the timeframe defined in the DBHG.

The Table below presents a detailed analysis of the timeframes (in calendar days) associated with each of the five breaches that involved notifications to individuals. As shown in the table, it took between 50 and 154 calendar days (an average of more than 3 months) after the FDIC discovered the incidents for the Corporation to complete the analysis of breach data and make a decision to notify the individuals involved. Further, it took an additional 145 to 215 calendar days (or 104 to 154 business days—an average of 6 months) for the FDIC to begin sending notification letters to potentially affected individuals. These breaches potentially affected over 113,000 individuals.

Table: Timing of Breach Notification Decisions and Notifications

	Date Breach Was Discovered	Date Decision Was Made to Notify	Days from Discovery to Notification Decision	Date Individuals Began to be Notified	Days from Notification Decision to Notifications Being Sent	Potentially Affected Individuals Notified
5	1/7/2016	5/12/2016	126	11/14/2016	186	11,417
6	2/29/2016	5/12/2016	73	11/15/2016	187	36,997
8	6/16/2016	8/5/2016	50	12/28/2016	145	19,287
10	1/11/2016	5/12/2016	122	11/11/2016	183	11,931
12	12/10/2015	5/12/2016	154	12/13/2016	215	33,969
Total						**113,601**

Source: OIG analysis of FDIC breach documentation.

Factors that Contributed to Untimely Breach Investigations and Notifications

The FDIC Did Not Have an Incident Response Coordinator

NIST guidance (SP 800-61) states that a single employee, with one or more designated alternates, should be in charge of incident response. However, the FDIC did not have such an individual—referred to as an Incident Response Coordinator—to centrally manage the Corporation's incident response strategy, plans, processes, procedures, activities, and resources. At the FDIC, the Incident Response Coordinator would have led the incident response workflow, including delegating assignments, and establishing milestones, deadlines, and timeframes for completion. ISPS and CIOO personnel that we spoke with acknowledged that had the FDIC designated a single Incident Response Coordinator, it

could have alleviated role confusion among ISMs and ISPS staff in responding to breaches, and improved the quality of information provided to the DBMT to support decision-making, thereby accelerating breach response activities.

The FDIC identified the need for an Incident Response Coordinator several years ago but did not hire an individual to serve in this role. Specifically, in November 2013, the FDIC conducted an internal exercise to explore the CIOO's readiness to respond to a cyber incident. The results of the exercise, which were incorporated into a document, entitled *Cyber Security Incident Response: A Management Priority 2013 Facilitated Discussion After Action Review* (the Incident Response Review), included eight recommendations to improve the FDIC's cyber incident capability. One of these recommendations was to appoint an incident coordinator.

In December 2016, FDIC engaged an independent, third-party firm (FDIC contractor) to complete an assessment of the FDIC's IT security and privacy programs, entitled the *Independent End-to-End Review of IT Security and Privacy Program* (End-to-End Security and Privacy Assessment). This assessment reiterated the need to identify and hire an Incident Response Coordinator. The review noted that establishing such a position was critical to modernizing the FDIC's incident response program and reducing the risk of inconsistent identification and remediation of security incidents.

We spoke with the individual who served as the FDIC's CISO between December 2013 and February 2016. This individual informed us that the FDIC had not hired an Incident Response Coordinator due to turnover at the CIO/CPO position. The current CIO/CPO informed us that he decided not to hire an Incident Response Coordinator in 2016 in order to consider the results of the End-to-End Security and Privacy Assessment. On April 14, 2017, the FDIC announced a position for an Incident Response Coordinator. As of the close of our audit fieldwork, the FDIC was considering potential candidates for the position.

ISMs Did Not Have Adequate Training

NIST guidance (SP 800-61) includes recommendations for organizing a computer security incident handling capability. One such recommendation is to select people with the appropriate skills for addressing incident response and provide them with necessary training. The NIST guidance states that deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data. It also states that without well-trained and capable staff, incident detection and analysis will be inefficient, and costly mistakes will result.

The FDIC had not established a role-based training program for the ISMs. The Incident Response Review conducted in November 2013 recommended that the FDIC develop a training and awareness program for ISMs to ensure consistent incident response handling across the FDIC's divisions and offices. However, the FDIC did not fully address this recommendation. More than 2 years later, in response to a recommendation we made in

October 2015,[17] the FDIC conducted an assessment of the ISM Program to determine whether the skills, training, oversight, and resource allocations pertaining to the ISMs enabled them to effectively carry out their responsibilities. The assessment results, which were detailed in a July 29, 2016 report, identified program gaps, including the need to establish a formal role-based training program for ISMs. The report indicated that 66 percent of ISMs surveyed rated their skill level in the role of incident response as intermediate or less than intermediate—a level the report indicated was lower than should be considered necessary for ISMs.[18]

CIOO officials informed us that, in their view, the DBMT should generally be able to determine an appropriate course of action to address a breach after one meeting. However, several DBMT members informed us that inadequate preparation on the part of ISMs resulted in the need for multiple DBMT meetings, which slowed breach investigations and response activities. We noted that of the five breaches we reviewed that involved notification to individuals:

- Two required multiple DBMT meetings to determine an appropriate course of action.

- One involved four DBMT meetings without a determination regarding an appropriate course of action. In this case, the CIO/CPO made a decision to notify individuals before the DBMT made its determination on a recommended course of action.

We describe how inaccurate or incomplete information in IRA forms affected the DBMT's ability to make informed decisions later in this report. Establishing a role-based training program for ISMs would help to ensure that information provided to the DBMT is complete and accurate.

Staffing to Support Breach Response Activities Was Not Sufficient

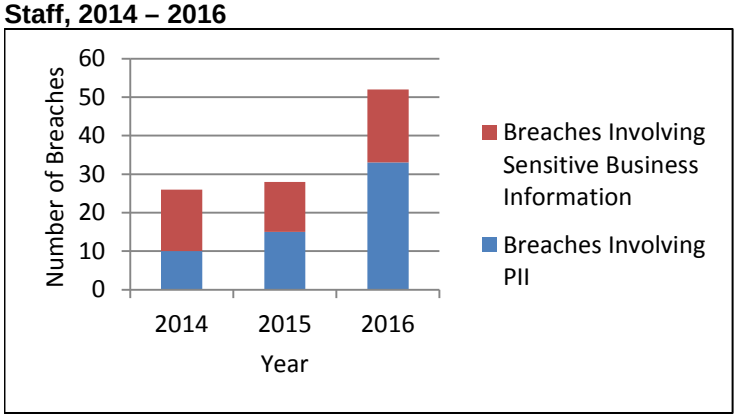
According to NIST guidance (SP 800-61), organizations should consider their staffing and resources when establishing an incident response capability. The ISM Program Assessment completed in July 2016 found that most ISMs did not have the ability or time to complete all tasks assigned to them, and some were severely overwhelmed. The assessment identified resource constraints as a top challenge for the ISM Program. ISPS personnel informed us that the FDIC planned to hire five additional ISMs by September 2017.

[17] See OIG Report, entitled *Audit of the FDIC's Information Security Program—2015* (Report No. AUD-16-001, dated October 2015).

[18] ISMs surveyed had the option to respond that they had a sophisticated understanding (Expert), thorough understanding (Thorough), intermediate understanding (Intermediate), basic understanding (Basic), or no sufficient knowledge (No Proficiency) in the specialty areas.

In addition, the End-to-End Security and Privacy Assessment completed by an FDIC contractor in December 2016 concluded that ISPS did not have adequate Privacy Staff to support breach response efforts and that this limitation contributed to delays in managing breaches. Figure 6 illustrates the number of business sensitive information incidents, classified by the FDIC as breaches,[19] and PII breaches handled by the Privacy Staff between 2014 and 2016. The CIOO decided in 2014 to task the Privacy Staff with responding to incidents involving business sensitive information, in addition to incidents involving PII. Further, in September 2015, the CIOO modified the configuration of the Corporation's data loss prevention (DLP) tool to begin monitoring the network for instances in which users copy sensitive data, including both PII and business sensitive information, to removable media. Between September 2015 and June 2016, the DLP tool flagged a total of 634,787 events involving the use of removable media. To determine whether the event had a legitimate business purpose, or warranted escalation to CSIRT for investigation, it required a manual review by an ISPS security specialist. We noted that 30 of the 634,787 events involving removable media were escalated by CSIRT to Privacy Staff, requiring a detailed investigation.

Figure 6: Number of Breaches Handled by FDIC Privacy Staff, 2014 – 2016



Source: OIG analysis of ISPS incident data.

While the Privacy Staff's workload significantly increased during 2016, its staffing level remained relatively constant. Further, we noted that the Privacy Program Manager position was vacant between November 2015 and September 2016—the same period during which the FDIC identified and began investigating the six major incidents we reviewed. In addition, a Privacy Staff employee was detailed on a part-time basis to another FDIC division in June 2016 for a 3-month period. ISPS and CIOO officials informed us that the increased workload among the Privacy Staff negatively affected the timeliness of breach investigation activities and increased the risk of mistakes.

[19] During the scope period of this audit, the DBHG defined the term data breach as an incident in which FDIC sensitive information, including business sensitive information and/or PII, has been lost, compromised, acquired, disclosed, or accessed without authorization, or any similar incident where persons other than authorized users and for other than authorized purposes have access or potential access to sensitive information. On April 7, 2017, the FDIC revised its definition of the term breach to only include incidents involving PII.

The FDIC Was Not Prepared To Handle a Large Volume of Notifications

For the calendar years 2013, 2014, and 2015, the FDIC notified a total of 1,746 individuals who were involved in PII-related breaches discovered by the Corporation. During 2016, the FDIC decided to notify over 140,000 individuals that their personal information had been involved in a breach and offer them identity and credit protection services, including credit monitoring, identity theft insurance, and identity restoration services. Although the FDIC had a contract in place to notify individuals and offer credit monitoring services, ISPS personnel informed us that the anticipated costs associated with the notification and credit monitoring effort in 2016 exceeded the value of that contract. ISPS personnel also informed us that they reviewed the terms of FDIC's existing contract against the General Services Administration's (GSA) Identity Protection Services (IPS) Blanket Purchase Agreement (BPA), effective September 1, 2015. The results of this review, together with the negative publicity associated with the OPM breach, prompted FDIC to procure a new credit monitoring contract through GSA's IPS BPA.

The new credit monitoring and identity theft protection services contract was awarded on June 28, 2016, approximately 1-1/2 months after the FDIC decided to notify potentially affected individuals. The new contract had a 2-year period of performance (with possible extensions) and a maximum value (ceiling price) of $13.3 million. ISPS personnel informed us that in the months following the award of the contract, FDIC division and office staff spent considerable time and effort:

- Researching current addresses of individuals potentially affected by the major incidents. Our review of ISPS records found that it took FDIC divisions, on average, 48 days to provide Privacy Staff with complete lists of potentially affected individuals for release to the credit monitoring contractor;

- Converting and formatting data into a structured format that the credit monitoring contractor could use to make notifications to potentially affected individuals; and

- Reaching agreement on the language that would be included in notification letters to potentially affected individuals and financial institutions.[20] Our review of ISPS records found that it took approximately 67 days for ISPS and divisions and offices to finalize the language in the notification letters for four of the five breaches that we reviewed that involved notification.

The FDIC began issuing notification letters to potentially affected individuals about 4-1/2 months (or 136 days) after the credit monitoring contract was awarded.

Recommendation

The FDIC took, or was working to take, a number of actions to address the weaknesses that caused the breach investigation activities and notifications to individuals to be untimely.

[20] Templates for notification letters are included in the DBHG.

Most notably, the FDIC Chairman approved the following priority initiatives in support of the Corporation's 2017 Performance Goals:

- Increase the effectiveness of the FDIC's cybersecurity risk management program by implementing the approved recommendations from the ISM Program Assessment completed in 2016. As part of this effort, the FDIC was working to develop a training plan for ISMs and establish teams to develop a role-based ISM education and training program in 2017.

- Implement approved recommendations from the End-to-End Security and Privacy Assessment completed in December 2016.

In addition, the FDIC completed a lessons-learned review of the FDIC's breach response and notification activities in May 2017. Further, the FDIC was working to hire an Incident Response Coordinator and five ISMs, and update its Breach Response Plan. Although these steps are positive, the FDIC needed to take the following additional action to address the remaining weaknesses identified during the audit.

We recommend that the CIO/CPO:

1. Allocate the appropriate level of FDIC resources, including Division and Office ISMs and Privacy Staff, to ensure that the FDIC can effectively meet its obligations with respect to breach response activities along with other workload requirements.

FDIC Did Not Adequately Document Key Assessments and Decisions

Our review of 18 suspected or confirmed breaches found that:

- The IRA forms did not clearly explain the rationale behind the overall impact/risk levels (i.e., High, Moderate, or Low) assigned to the breaches;

- Some IRA forms were not substantially complete prior to convening the DBMT;

- The underlying analyses used to support the assigned impact/risk levels for three breaches was not consistent with the methodology in the DBHG; and

- The overall risk ratings recorded in the IRA forms for five breaches were inconsistent with the risk mitigation actions taken by the FDIC.

The overall impact/risk level assigned to a breach is critically important because the FDIC uses it to determine an appropriate course of action, such as whether potentially affected individuals will be notified and the speed of the notifications, to mitigate the risk of a breach. Inaccurate impact/risk factor ratings may cause the FDIC not to implement

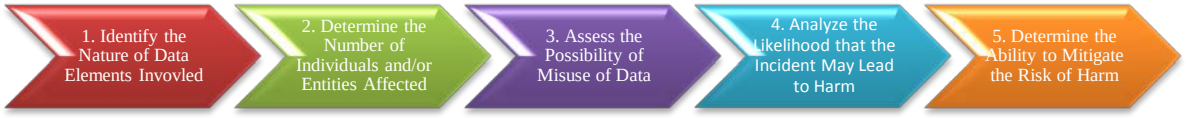
appropriate risk mitigation actions, exposing consumers to increased risk of harm. In addition, IRA forms serve as investigative records and, as such, must contain reliable information to protect the FDIC's business and legal interests.

Further, inaccurate or incomplete information in IRA forms limits the ability of DBMT members to effectively evaluate the risk of harm to individuals and, therefore, delays decision-making. In addition, not documenting a clear rationale for overall impact/risk ratings and decisions regarding notifications and offering services to potentially affected individuals makes it difficult for the FDIC to establish precedent in an effort to promote consistency in the process. In other words, if the FDIC had properly recorded its decision-making process, decisions about future breaches could be evaluated against past examples to help ensure consistency in the FDIC's breach response efforts.

Assessing the Risk of Harm

The DBHG states that the five-factor risk analysis methodology depicted in Figure 7 shall be followed when assessing the likely risk of harm caused by a breach and determining an appropriate course of action. The methodology is based on OMB guidance and NIST risk assessment guidelines that utilize the impact levels of High, Moderate, and Low to rate the potential harm that could result if PII were inappropriately accessed, used, or disclosed. According to the DBHG, the ISPS Incident Lead and ISM work together to assign an impact/risk level rating for each of the five factors. These officials then "balance the five factors collectively" to assign an overall impact/risk level rating of High, Moderate, or Low for the breach. These ratings are recorded in the IRA form. In cases where the DBMT is convened, it reviews and validates the impact/risk level ratings and recommends risk mitigation actions, which may include external breach notifications and/or services to potentially affected individuals. The DBHG states that the decision to provide notification should give greater weight to Factor 3 (*Possibility of Misuse of Data*) and Factor 4 (*Likelihood the Incident May Lead to Harm*).

Figure 7: The Five-Factor Incident Risk Analysis Methodology



Source: The DBHG, Versions 1.4 dated April 16, 2015 and 1.5 dated June 6, 2016 (the versions in effect for the period covered by the audit).

GAO, in its report entitled *Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, dated December 2013, recommended that the FDIC document the reasoning behind its risk determinations for breaches involving PII. In response to GAO's recommendation, the FDIC updated its breach procedures to include an Incident Risk Analysis and Impact Assessment (i.e., the IRA form) to facilitate a greater understanding of the FDIC's risk determinations. However, our review of IRA forms found

that they did not clearly describe how the FDIC determined the overall impact/risk rating for 13 of the 14 confirmed breaches in our sample. For example:

- One breach involved the compromise of PII for approximately 22,000 individuals. The IRA indicated that three of the five factors (i.e., the *Nature of the Data Elements Involved*, the *Likelihood the Incident May Lead to Harm*, and the *Ability to Mitigate the Risk of Harm*) were rated Moderate. However, the overall impact/risk level rating was Low. As discussed above, the DBHG states that the decision to provide notification should give greater weight to certain factors, including the *Likelihood the Incident May Lead to Harm*.

- Another breach involved the compromise of PII for approximately 20,000 individuals. Because the breach included full names, SSNs, and home addresses for the individuals involved, the *Nature of the Data Elements Involved* factor was rated as High. However, the overall impact/risk rating was Low.

In addition, we determined that IRA forms for four of the breaches we reviewed were not substantially complete prior to convening the DBMT. For example:

- The IRA form for one confirmed breach identified the answers to many of the questions in the impact/risk assessment regarding the *Possibility of Misuse of Data* and *Likelihood the Incident May Lead to Harm* factors as "unknown." According to the DBMT meeting minutes for this breach, the risk level was not determined at the conclusion of the meeting.

- The DBMT meeting minutes for another confirmed breach stated that a key follow-up action item was to review data files to determine their content, including the identification of PII, even though the *Nature of the Data Elements Involved* factor is part of the incident risk analysis methodology and the ISPS Incident Lead and ISM are required to complete it prior to the DBMT meeting.

We also identified three IRA forms that contained one or more impact/risk factor ratings that were inconsistent with the methodology defined in the DBHG. Specifically, the DBHG states that if a breach involves certain types of PII, such as SSNs, the *The Nature of the Data Elements Involved* factor should be rated as High. Although these three IRA forms stated that such PII was involved in the breaches, the impact ratings for the *Nature of the Data Elements Involved* factor were all Low.

We attributed the weaknesses described above to two causes. First, the DBHG did not require staff to document the rationale behind the overall impact/risk level ratings assigned to breaches. Secondly, as previously discussed, the FDIC had not established formal role-based training for its ISMs that would have helped to ensure the consistent assessment of risk for breaches involving PII.

Finally, we noted that the IRA forms for five of the six major incidents involving notification to over 113,000 individuals reflected an overall impact/risk level rating of "Low." However, the IRA forms for these five breaches did not explain how the overall risk ratings were determined. As mentioned earlier in the report, the DBMT originally determined that the risk was low for three of the five breaches and based on mitigating factors, notification and credit monitoring to potentially affected individuals would not occur. The IRA forms for these breaches included a notation stating, "As per the CIO's direction on May 12, 2016, notification and credit monitoring will be provided to parties potentially affected by this incident." The IRA forms for these breaches did not provide an explanation of the rationale for this decision or change from the DBMT's original conclusions. Ultimately, the FDIC notified 60,345 potentially affected individuals in response to these breaches.

For another of the five breaches, the FDIC generally documented within the IRA form that the DBMT had decided out of an abundance of caution to provide notification and credit monitoring to potentially affected individuals. For the remaining breach, the DBMT had not yet made a decision about whether to notify or offer services to potentially affected individuals when the CIO/CPO decided on May 12, 2016 that potentially affected individuals would be notified.[21] Although the decision to notify was captured on the IRA form for this breach, the rationale for the decision was not documented. Consequently, the overall impact/risk ratings in the IRA forms we reviewed were inconsistent with the FDIC's mitigation actions. Without properly recording the decision-making process and rationale for breach response decisions, it is difficult for the FDIC to benchmark against future breaches and ensure consistency in its processes.

Inaccurate or incomplete information in IRA forms limits the ability of the DBMT (when convened) to review and concur with an ISM's and ISPS Incident Lead's assessment of the risk of harm and reach consensus on a recommended course of action to mitigate potential harm. During our discussions with DBMT members aimed at gaining an understanding of areas for improvement within the breach response process, we were informed that IRA forms provided to them for decision-making were not always complete (e.g., did not always contain accurate or updated information on the number of individuals or entities potentially affected by the breach or did not always contain completed risk assessments, including ratings for each of the five factors and an overall impact/risk rating).

Recommendation

The FDIC was taking a number of actions to address the underlying causes that contributed to the weaknesses described above. Such actions include the establishment of plans to provide role-based training for ISMs and actions to address a prior OIG recommendation to

[21] As described earlier in this report, we spoke with the FDIC Chairman, Chief Operating Officer, and CIO/CPO to obtain an understanding of the rationale for this decision.

update the FDIC's incident response policies, procedures, and guidelines[22] to ensure, among other things, that:

- Documentation related to investigation activities and decision-making is recorded, dated, and centrally maintained;

- IRA forms contain up-to-date information throughout the investigation supported by appropriate evidence; and

- The underlying analyses for key decisions are adequately documented.

The FDIC needs to take the following additional action to address the remaining weaknesses identified during the audit.

We recommend that the CIO/CPO:

2. Establish a procedure that requires the FDIC to explain its rationale, in written form, justifying the overall impact levels assigned to breaches.

FDIC Needed to Strengthen Controls Over the DBMT

The DBMT plays a critical role in determining and managing the FDIC's response activities for significant breaches involving PII. Specifically, the DBMT's responsibilities include:

- Reviewing and approving the incident impact/risk assessment prepared by the ISM and ISPS Incident Lead that addresses the risk of harm posed to affected individuals/entities, the financial sector (if applicable), and the Corporation;

- Determining and managing an appropriate course of action in response to breaches and mitigating potential harm; and

- Recommending appropriate external breach communications and notifications, including notifications to affected individuals, banks, or other entities, to the FDIC CIO/CPO (or designee) for approval.

Although the DBHG describes the role and activities of the DBMT, the FDIC had not established a formal charter or similar mechanism for the DBMT that defines its purpose, scope, governance structure, and key operating procedures. Key operating procedures include, for example, the processes by which the DBMT validates the impact/risk assessment prepared by the ISM and selects a recommended course of action for mitigating

[22] This recommendation, which was not fully implemented at the close of our fieldwork, was contained in our report, entitled *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*, (Report No. AUD-16-004, dated July 2016 and updated February 2017).

the risk; makes decisions (e.g., formal vote or consensus); resolves disagreements among members; and prepares and maintains key documentation, such as meeting minutes.

Establishing charters is a common business practice at the FDIC. For example, the FDIC recently established a charter for its Access Control Program (ACP) that defines its purpose, scope, and governance structure. The ACP charter also establishes procedures that define how the ACP program will operate, including how items are voted on and resolved when consensus cannot be reached. Such governance mechanisms help to ensure that roles, responsibilities, and expectations of stakeholders are clear, thereby mitigating role confusion. One of the DBMT members that we spoke with indicated that although the meetings have recently become more organized, there was general confusion regarding the roles and responsibilities of those attending DBMT meetings held in 2016.

The FDIC had also not developed a process for briefing the DBMT on the final findings of investigations and the actions taken in response to DBMT recommendations to resolve breach events. Notably, for 3 of the 18 incidents we reviewed, the DBMT made a recommendation not to notify potentially affected individuals that their personal information was involved in a breach. However, the CIO/CPO subsequently decided to notify those individuals. The DBMT did not formally meet to discuss the reasons for this change in direction, or its implications for future DBMT deliberations and decisions. Developing a process for briefing the DBMT on the outcome of its recommended actions would allow DBMT members to more effectively leverage lessons-learned for future breach response decision-making and promote greater consistency in the process.

Further, the FDIC had not provided DBMT members with specialized training to help ensure the successful implementation of their responsibilities. The need for specialized training for DBMT members was identified in the 2013 Incident Response Review but had not been addressed. Recent OMB guidance stresses the importance of training key members of the breach response team. Specifically, OMB Memorandum M-17-12 issued in January 2017 states that the SAOP shall periodically, but not less than annually, convene the agency's breach response team to hold a tabletop exercise. Tabletop exercises serve to test the breach response plan and help ensure the members of the response team are familiar with the plan and understand their specific roles.

Recommendations

In light of the critically important role that the DBMT plays in the breach response process, we recommend that the CIO/CPO:

3. Establish a charter or similar mechanism for the DBMT that defines its purpose, scope, responsibilities, membership, governance structure, and operations.

4. Develop and implement a process for briefing the DBMT on the final findings of breach investigations and the actions taken in response to DBMT recommendations to resolve breach events.

5. Provide specialized training for DBMT members that includes tabletop exercises to ensure they fully understand and consistently implement their roles and responsibilities.

FDIC Did Not Track and Report Key Breach Response Metrics

NIST guidance (SP 800-61) states that organizations should have an incident response plan that includes, among other things, metrics for measuring and evaluating the effectiveness of incident response. According to the NIST guidance, metrics can be useful for identifying trends and systemic weaknesses, analyzing the adequacy of control activities, and monitoring the accomplishment of goals and objectives. The DBHG states that metrics provide a frame-of-reference for gauging and benchmarking the overall efficiency and effectiveness of the FDIC's breach prevention and response capabilities, while driving operational improvement and enhancing data safeguards.

The DBHG identifies key categories of qualitative and quantitative metrics designed to benchmark, tailor, and continuously improve the FDIC's breach prevention and response capabilities. However, the FDIC generally did not track or report key breach response metrics for the 18 suspected or confirmed breaches that we reviewed. For example, as detailed in Figure 4 of this report, the DBHG identified reporting and response timelines as a key metric and established specific timeframes for completing key breach response activities. With the exception of reporting incidents to US-CERT within 1 hour, the FDIC did not track or report these metrics for the incidents we reviewed. Further, as discussed earlier in this report, the FDIC generally did not meet the metrics we reviewed.

The DBHG also identified cost efficiency, including the cost of response efforts and credit monitoring, as a key metric. However, the FDIC did not track or report the cost of its breach response efforts for the incidents we reviewed. According to ISPS officials, the timeframes established within the DBHG were viewed as guidelines rather than required metrics for performance. Further, the FDIC did not record when key investigative activities were completed for the incidents we reviewed. Such information is needed to assess actual performance against the metrics in the DBHG. Our review of IRA forms for the 18 suspected or confirmed breaches found that the IRAs did not reflect the dates of:

- The completion of impact/risk factor determinations (including overall impact/risk determinations);
- The determination that the incident constituted a breach; or
- The decision to close out the incident or breach investigation.

At the time of our audit, ISPS officials also informed us that the Combined Operational Risk, Security, Investigation, and Compliance Application (CORSICA)—the FDIC's system of record for tracking and managing incidents—did not yet have the functionality

that would allow for the reporting of key metrics. Prior to the implementation of CORSICA in July 2016, the FDIC did not centrally store and track incident information and supporting documents. The lack of centralized records further limited the FDIC's ability to track and report key metrics. ISPS officials informed us they planned to implement improved functionality in CORSICA to track key metrics.

The FDIC needs to begin collecting, analyzing, and reporting breach response metrics to support management decision-making. For example, tracking the hours and costs associated with response activities could help management better assess whether its resource commitments are adequate. In addition, measuring the amount of time it takes to complete breach investigation activities could help to identify areas warranting management attention or control improvements. Absent effective metrics, FDIC managers and other stakeholders lack timely, action-oriented information needed to assess program performance and ensure accountability.

Recommendation

We recommend that the CIO/CPO:

6. Establish, track, and report metrics to assess the performance of breach response activities.

FDIC Needs to Update Its CPO Designation to Reflect Current Organizational Responsibilities

We identified an other matter that, although not within the scope of the audit, warrants management attention. Specifically, the FDIC needed to update its written CPO designation to reflect organizational changes that have occurred since the original designation was made in March 2005. A brief summary follows.

In a memorandum dated March 9, 2005, the FDIC Chairman designated the CIO, who at that time also served as the FDIC's Director, DIT, to be the Corporation's CPO. The March 2005 memorandum states:

> *Pursuant to authority granted to me as Chairman, I do hereby designate the Chief Information Officer and Director, Division of Information Technology, also to serve as Chief Privacy Officer of the Federal Deposit Insurance Corporation, with responsibility for those duties assigned to that position by law and by administrative action, and with overall agency-wide responsibility for information privacy issues.*
>
> *This designation shall remain in effect until revoked or modified.*

The FDIC Chairman made this designation in response to requirements in Section 522 and guidance in OMB Memorandum M-05-08, *Designation of Senior Agency Officials for*

Privacy, dated February 11, 2005. The statute and OMB guidance required federal agencies to designate a senior agency official with overall responsibility for privacy. In July 2013, the FDIC separated the roles and responsibilities of the CIO and Director, DIT. These positions are now held by different individuals.

On September 15, 2016, OMB issued Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*. OMB Memorandum M-16-24 directed federal agency heads to assess the management, structure, and operation of their agency's privacy programs and, if necessary, designate or re-designate a new official to serve as the SAOP. In response to this guidance, the FDIC completed an internal evaluation in November 2016. This evaluation found that "the FDIC Privacy Program in its current form is compliant with existing law and OMB guidance. Furthermore, given the Chairman's 2005 designation of the CIO to serve as the FDIC's CPO (as well as the identical nature of the CPO and senior agency official for privacy roles at the FDIC), there is nothing further to be done concerning designation (or re-designation) of the senior agency official for privacy/CPO."

We noted, however, that the internal assessment did not address the separation of the CIO and DIT Director positions that were made in July 2013. To ensure clarity of responsibilities, the FDIC should update its formal CPO designation to reflect this change.

Recommendation

We recommend that the CIO/CPO:

7. Coordinate with the FDIC Chairman to update the CPO designation to reflect organizational changes made since 2005.

Corporation Comments and OIG Evaluation

The CIOO provided a written response, dated September 25, 2017, to a draft of this report. The response is provided in its entirety in Appendix 4. In the response, FDIC management concurred with all seven of the report's recommendations. Management's planned corrective actions for the seven recommendations will remain open until we confirm that corrective actions have been completed. A summary of the Corporation's corrective actions is presented in Appendix 5.

Objective, Scope, and Methodology

Objective

The audit objective was to assess the adequacy of the FDIC's processes for (1) evaluating the risk of harm to individuals potentially affected by a breach involving PII and (2) notifying and providing services to those individuals, when appropriate.

We conducted this performance audit from August 2016 through June 2017 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 20, 2017.

Scope and Methodology

To address the audit objective, we reviewed relevant provisions of federal statutes and government-wide policy and guidance issued by OMB and NIST related to the handling of breaches. Specifically, we identified and reviewed:

Relevant Statutes

- The FISMA legislation
- The Privacy Act of 1974

OMB Policy and Guidance

- Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*
- Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*
- Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*

NIST Guidance

- SP 800-61, Revision 2, *Computer Security Incident Handling Guide*
- SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

We also considered GAO's *Standards for Internal Control in the Federal Government*. In addition, we reviewed the FDIC breach response policies, procedures, and guidance, including:

- The *Data Breach Handling Guide*, Version 1.4, dated April 16, 2015; and Version 1.5, dated June 6, 2016
- Circular 4010.3, *FDIC Enterprise Risk Management Program*, dated April 16, 2012
- Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007
- Circular 1360.12, *Reporting Computer Security Incidents*, dated April 7, 2017
- Circular 1360.20, *FDIC Privacy Program*, dated March 13, 2017

Further, we interviewed FDIC personnel who had responsibility for conducting breach investigations and notifying potentially affected individuals to discuss their roles, responsibilities, and perspectives for both specific incidents as well as the FDIC's incident response program as a whole. Such personnel included:

- The CIO/CPO
- The current and former CISO
- The former Acting Privacy Program Manager
- ISPS Incident Leads
- Selected ISMs
- Legal Division staff familiar with the DBMT process
- Selected members of the DBMT

We reviewed the FDIC's investigative records and activities for 18 suspected or confirmed breaches of PII to assess the manner in which the FDIC evaluated the risk of harm to potentially affected individuals and notified and provided services, when appropriate. We judgmentally selected the 18 incidents from a universe of 54 suspected or confirmed breaches involving PII that the FDIC discovered during the period January 1, 2015 through December 1, 2016. Because we did not use statistical techniques to select the 18 incidents, the results of our analysis cannot be projected to the population.

ISPS initially provided us with a universe of suspected or confirmed breaches of PII for the time period referenced above on December 8, 2016. We corroborated the universe to the extent possible with information from other sources, such as documentation from a prior FDIC OIG audit and testimonial evidence, and determined that the universe was not complete. We brought this matter to the attention of ISPS and were provided with a new universe of suspected or confirmed breaches on January 10, 2017. We spoke with ISPS personnel to gain an understanding of how the universe was developed and why the initial universe provided to us was not complete. In doing so, we were able to assure ourselves

that the information provided to us on January 10, 2017 was sufficiently reliable for the purposes of our work.

We chose the 18 suspected or confirmed breaches in such a manner as to obtain representation from multiple FDIC divisions, breaches that required notification to individuals, and breaches of both physical and electronic records. For each of these suspected or confirmed breaches, we reviewed key investigative records and activities to determine whether: they constituted a breach as defined in FDIC policy and guidance; the FDIC assessed and documented the risk of harm in accordance with the DBHG; and the FDIC notified potentially affected individuals that their personal information was involved in a breach in a timely manner.

Throughout our audit, the FDIC updated its breach response policies, procedures, and guidelines to address new guidance issued by OMB and to improve the Corporation's breach response controls. We evaluated the FDIC's response activities for the 18 suspected or confirmed breaches against the policies, procedures, and guidelines that were in effect at the time the FDIC discovered and addressed the breaches. We considered new guidance issued by OMB and relevant updates to the FDIC's policies, procedures, and guidelines when developing our findings, conclusions, and recommendations.

Regarding compliance with laws and regulations, we assessed the FDIC's compliance with relevant provisions of FISMA and OMB memoranda as it pertains to evaluating the risk of harm to individuals potentially affected by a breach of PII and notifying and providing services, when appropriate. The results of our assessments are described throughout this report. In addition, we assessed the risk of fraud and abuse related to the audit objective in the course of evaluating audit evidence. We performed our work at the FDIC's Headquarters offices in Washington, D.C., and Virginia Square offices in Arlington, Virginia.

Glossary of Terms

Term	Definition
Credit Monitoring	A commercial service that can assist individuals in the early detection of identity theft. A credit monitoring service typically notifies individuals of changes that appear in their credit reports, such as the creation of new accounts and inquiries of credit by merchants.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or similar occurrence where (1) a person 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.
Data Loss Prevention Tool	Software designed to detect and, if enabled, prevent potential data breaches by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
Identity Theft Insurance	Generally provides reimbursement for the cost of restoring a victim's identity and repairing their credit reports.
Incident	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information Security Manager (ISM)	ISMs are located within FDIC divisions and offices and provide a business focus on information security and coordinate with the CIOO to ensure that appropriate security controls are in place to protect their respective division or office's information and information systems. ISMs are responsible for such things as educating employees and contractors on how to properly safeguard FDIC information; assessing system security levels; ensuring that security requirements are addressed in new and enhanced systems; and promoting compliance with security policies and procedures.
Major Incident	An incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. OMB Memorandum M-17-05 provides agencies with a framework for assessing whether an incident is major.

Glossary of Terms

Term	Definition
Personally Identifiable Information (PII)	Any information about an individual that can be used to distinguish or trace that individual's identity, such as their full name, home address, e-mail address (non-work), telephone numbers (non-work), SSNs, driver's license/state identification number, EIN, date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, or personal identification number), medical information, investigation report or database, criminal or employment history or information, or any other personal information which is linked or linkable to an individual.

Acronyms and Abbreviations

Acronym/Abbreviation	Explanation
ACP	Access Control Program
BPA	Blanket Purchase Agreement
BRP	Breach Response Plan
BRT	Breach Response Team
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISO	Chief Information Security Officer
CORSICA	Combined Operational Risk, Security, Investigation, and Compliance Application
CPO	Chief Privacy Officer
CSIRT	Computer Security Incident Response Team
DBHG	Data Breach Handling Guide
DBMT	Data Breach Management Team
DIT	Division of Information Technology
DLP	Data Loss Prevention
EIN	Employee Identification Number
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
FTC	Federal Trade Commission
GAO	Government Accountability Office
IPS	Identity Protection Services
IRA	Incident Risk Analysis
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	Personally Identifiable Information
POC	Point of Contact
SAOP	Senior Agency Official for Privacy
Section 522	Section 522 of Division H of the Consolidated Appropriations Act, 2005, as amended
SP	Special Publication
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team

Corporation Comments

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

DATE: September 25, 2017

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

THROUGH: Lawrence Gross, Jr. **/Signed/**
Chief Information Officer and Chief Privacy Officer

FROM: Howard Whyte **/Signed/**
Chief Information Security Officer

SUBJECT: Management Response to the Draft Audit Report Entitled *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (Assignment No. 2016-041)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* issued August 25, 2017. Cybersecurity 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 is a top priority at the FDIC.

In its report, the OIG reviewed a total of 18 breaches all of which were discovered between January 1, 2015, and December 1, 2016. Six of the 18 breaches were designated as "major" as defined in previous OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015.[1] The FDIC has made significant progress to strengthen the agency's cybersecurity posture and is continuously working to improve our Breach Response Program under the replaced guidance OMB issued in November 2016.

We appreciate your staff's time and effort and we expect that the actions taken in response to this draft report will further enhance the FDIC's IT Privacy controls, improve breach response processes and decisions, and reduce risk to the agency. This response outlines the Chief Information Officer Organization's (CIOO) planned corrective actions. We have carefully considered and concur with all seven recommendations. Our detailed response is organized by recommendation and contains actions already completed, planned, or in process.

[1] OMB subsequently revised the definition of major incident in Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, dated November 4, 2016.

Corporation Comments

MANAGEMENT RESPONSE

Recommendation 1 - Allocate the appropriate level of FDIC resources, including Division and Office ISMs and Privacy Staff, to ensure that the FDIC can effectively meet its obligations with respect to breach response activities along with other workload requirements.

Management Decision: Concur

Corrective Action:

FDIC has been conducting an ongoing assessment of the Privacy Program's workload and its commensurate level of resources. FDIC mapped its Privacy Program's processes, procedures and policies to the new A-130 privacy standards[2] in order to inform workforce planning. Over the past several months, we have increased resources to the Privacy Staff; allocating twenty five percent more federal staff and forty percent more contractors to ensure that the FDIC can more effectively meet its breach response obligations as well as other privacy functions. The Privacy Staff has and continues to increase its allocated contracting resources to plan for and implement new breach response activities. Additionally, the Office of the Chief Information Security Officer was reorganized to elevate the Privacy Staff into a formal Section that will be led by a *Privacy Section Chief*, reporting directly to the Chief Information Security Officer. This reorganization was approved in August 2017. Furthermore, the new permanent *Incident Response Coordinator* started on September 18, 2017, and we have been interviewing candidates for an *Information Security Manager Lead* with a target selection date of September 29, 2017.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

See corrective action plan description above.

Estimated Completion Date: April 9, 2018

[2] The Office of Management and Budget (OMB) revised Circular A-130, "Managing Information as a Strategic Resource," on July 28, 2016. The revised Circular emphasizes the role of both privacy and security in the Federal information life cycle. Importantly, it represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at Federal agencies.

Corporation Comments

Recommendation 2 - Establish a procedure that requires the FDIC to explain its rationale, in written form, justifying the overall impact levels assigned to breaches.

Management Decision: Concur

Corrective Action:

The new version of the Breach Response Plan (BRP) incorporates guidance from Memorandum OMB M-17-12[3] and is currently being reviewed by stakeholders and provides a consistent, repeatable process for assigning impact levels of breaches to the risk of harm to individuals. Once published, the impact levels and rationale will be documented in CORSICA for each breach. CIOO will publish the new BRP and document the impact levels in CORSICA by December 8, 2017.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

The new process for assigning the risk of harm level to individuals for each breach will reduce the risk of this practice not being consistent or repeatable.

Estimated Completion Date: December 8, 2017

Recommendation 3 - Establish a charter or similar mechanism for the DBMT that defines its purpose, scope, responsibilities, membership, governance structure, and operations.

Management Decision: Concur

Corrective Action:

Per Memorandum OMB M-17-12, the new version of the BRP (which is currently being reviewed by stakeholders) defines the Breach Response Team (BRT) (formerly known as the Data Breach Management Team or DBMT) and includes its purpose, scope, responsibilities, membership, and governance structure. Basic operating procedures are included in the BRP. FDIC will continue to detail, refine, and improve existing standard operating procedures. Additionally, we will develop and present a memorandum for the Chairman's review and signature designating the BRT members concurrently with the BRP publication.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

[3] Memorandum OMB-17-12 was released in January 2017, and sets forth the policy for federal agencies to prepare for and respond to a breach of personally identifiable information. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes. While promoting consistency, this Memorandum also provides agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

3

Corporation Comments

The new BRP, along with designation memorandum, will meet the intent of this recommendation without the need for a separate formal written charter.

Estimated Completion Date: December 8, 2017

Recommendation 4 - Develop and implement a process for briefing the DBMT on the final findings of breach investigations and the actions taken in response to DBMT recommendations to resolve breach events.

Management Decision: Concur

Corrective Action:

The new version of the BRP (currently being reviewed by stakeholders) includes a new process and templates for capturing and communicating the final findings of the breach investigation, as well as the recommendations, decisions, and actions related to breach risk of harm assessments, including but not limited to, a Breach Report for documenting the final investigation and mitigation activities; a Breach Risk of Harm Assessment to document BRT recommendations; a new requirement that BRT discussions and recommendations be documented real-time in CORSICA during the BRT meeting, as well as that an Executive Summary (using a standard template) be prepared to summarize and track the BRT's recommendation and the Senior Agency Official for Privacy's (SAOP) concurrence/non-concurrence, and the final determination made by the head of the agency when applicable. The final Executive Summary of the breach will be provided to the BRT members at the conclusion of the breach response process. The new templates will be completed concurrent with the publication of the new BRP.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

See corrective action plan description above.

Estimated Completion Date: December 8, 2017

Recommendation 5 - Provide specialized training for DBMT members that includes tabletop exercises to ensure they fully understand and consistently implement their roles and responsibilities.

Management Decision: Concur

Corrective Action:

The new version of the BRP (currently being reviewed by stakeholders) requires role-based training for the BRT (formerly DBMT) and an annual tabletop exercise for the BRT members. As noted above, the current goal for the publication of the new BRP is

Corporation Comments

December 8, 2017. Further, Privacy has engaged Corporate University to assist with developing and conducting the BRT tabletop exercise by September 2018. Consistent with Memorandum OMB M-17-12, training will be delivered within one year of the tabletop exercise. Privacy is developing a training plan, including resources and funding, to develop and execute role-based training for the BRT (as well as role-based training for multiple other stakeholders as required by Memorandum OMB M-17-12). Delivery of the role-based privacy training courses is targeted for June 30, 2018.

Timeline:

BRP Completed => December 2017
Role-Based Training Completed => June 2018
Tabletop Exercise Completed => September 2018

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

See corrective action above; this training will be required under the new BRP.

Estimated Completion Date: September 30, 2018

Recommendation 6 - Establish, track, and report metrics to assess the performance of breach response activities.

Management Decision: Concur

Corrective Action:

The new version of the BRP (currently being reviewed by stakeholders) requires certain metrics related to the breach response process to be tracked and reported, in accordance with Memorandum OMB M-17-12. Additionally, the Privacy team has been working with the CORSICA implementation team to add additional tracking options over the past year to assist with assessing the performance of breach response activities. The current goal is for CORSICA to go live with additional tracking functionality by November 1, 2017 for Phase 1, and completion of the remaining Phases by April 9, 2018.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

See corrective action above; additional tracking functionality is currently being built into CORSICA to assist with assessing the performance of breach response activities.

Estimated Completion Date: April 9, 2018

Recommendation 7 - Coordinate with the FDIC Chairman to update the CPO designation to reflect organizational changes made since 2005.

5

Corporation Comments

Management Decision: Concur

Corrective Action:

The FDIC will update its written Chief Privacy Officer (CPO) designation to reflect organizational changes that have occurred since the original designation was made in March 2005. In detail, we will update the "Designation of Chief Privacy Officer" memorandum dated March 9, 2005, currently located on the Legal intranet site https://fdicnet.fdic.gov/content/dam/legal/documents/delegations-authority/chairman/chairCPO2005.pdf to accurately state that the CIO is the CPO as designated by the FDIC Chairman. We will therefore remove the "Director of DIT" title from the memorandum.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

The Office of Management and Budget's records indicate that the CIO is currently the Senior Agency Official for Privacy.

Estimated Completion Date: December 15, 2017

Any questions regarding this response should be directed to Kim Farrell at (703) 516-5101.

cc: James Anderson, Acting Deputy Director, DOF, Corporate Management Control Branch
Russell G. Pittman, Director, DIT
Renita K. Anderson, Deputy Director, DIT, Business Administration Branch
Rack D. Campbell, Chief, DIT, Audit and Internal Control Section
Shannon Dahn, Privacy Program Manager, Office of the CISO

6

Summary of the Corporation's Corrective Actions

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	FDIC will complete an assessment of the Privacy Staff's workload and associated resources. In recent months, the FDIC increased the amount of federal staff and contractor personnel dedicated to privacy. Further, in August 2017, the FDIC established the Privacy Staff as a section that will be led by a Privacy Section Chief, who will report directly to the CISO. In addition, the FDIC hired a permanent Incident Response Coordinator on September 18, 2017, and will hire an Information Security Manager Lead.	4/9/2018	No	Yes	Open
2	The FDIC will revise the BRP to incorporate guidance in OMB Memorandum M-17-12 and reflect a consistent process for assigning impact/risk levels for breaches. After the BRP is published, the impact/risk levels and associated rationale will be documented in CORSICA.	12/8/2017	No	Yes	Open

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
3	The FDIC will revise the BRP to define the purpose, scope, responsibilities, membership, governance structure, and basic operating procedures of the Breach Response Team (BRT), formerly known as the DBMT. In addition, the Chairman will formally designate the BRT members.	12/8/2017	No	Yes	Open
4	The FDIC will issue a revised BRP that includes a new process and templates for capturing and communicating the final findings of breach investigations, as well as the recommendations, decisions, and actions related to breach risk of harm assessments. The BRP will require that an Executive Summary be prepared that summarizes and tracks the BRT's recommendation(s), the SAOP's concurrence or non-concurrence, and the final determination made by the agency head, when applicable. The final Executive Summary will be provided to the BRT at the conclusion of the breach response process.	12/8/2017	No	Yes	Open
5	The FDIC will issue a revised BRP that requires role-based training and annual tabletop exercises for the BRT. In addition, the Privacy Staff will develop a training plan for stakeholders, including the BRT. Further, the FDIC will complete role-based training and a tabletop exercise for the BRT.	9/30/2018	No	Yes	Open

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
6	The FDIC will issue a revised BRP that requires the tracking and reporting of certain metrics related to the breach response process consistent with OMB guidance. The FDIC will also modify CORSICA to add new functionality to support breach response metric reporting.	4/9/2018	No	Yes	Open
7	The FDIC will update its written CPO designation to reflect organizational changes that have occurred since the original designation was made in March 2005.	12/15/2017	No	Yes	Open

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

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.