Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-16-005

The Cybersecurity Act of 2015—The FDIC's Controls and Practices Related to Covered Systems

August 2016

Office of Inspector General

Executive Summary

The Cybersecurity Act of 2015—The FDIC's Controls and Practices Related to Covered Systems

Report No. AUD-16-005
August 2016

Why We Did The Audit

On December 18, 2015, the President signed the Cybersecurity Act of 2015 into law. Among other things, the statute requires the Inspector General of each federal agency that operates a national security system or a computer system that provides access to personally identifiable information (PII)—collectively referred to herein as "covered systems"—to submit a report to the appropriate committees of jurisdiction in the United States Senate and the House of Representatives. In general, the report is to contain information collected from the agency on various computer security-related topics pertaining to covered systems.

The objective of the audit was to describe the FDIC's information security policies, procedures, practices, and capabilities for covered systems as prescribed by Section 406 of the Cybersecurity Act of 2015. Consistent with the provisions of the statute, the audit generally did not include an assessment of the adequacy of the FDIC's information security controls over covered systems. We engaged the professional services firm of Cotton & Company LLP (C&C) to conduct the audit.

Background

Section 406, *Federal Computer Security*, of the Cybersecurity Act of 2015 states that the report submitted by the Inspector General shall include a description of the:

- logical access policies and practices used by the agency to access a covered system, including whether appropriate standards were followed;
- logical access controls and multi-factor authentication used by the agency to govern access to covered systems by privileged users, and if such measures are not being used, the reasons why;
- policies and procedures followed to conduct inventories of the software present on covered systems and the licenses associated with such software;
- capabilities utilized by the agency to monitor and detect exfiltration and other threats, including data loss prevention, forensics and visibility, or digital rights management (including, if applicable, the reasons for not using the three referenced capabilities); and
- policies and procedures with respect to ensuring that entities, including contractors, that provide services to the agency are implementing certain information security management practices described above.

Audit Results

As of May 2016, the FDIC had 269 information systems that met the definition of a covered system. Consistent with the Cybersecurity Act of 2015, C&C's report describes the FDIC's information security policies, procedures, practices, and capabilities for these systems.

With respect to logical access to covered systems, the report notes that the policies C&C reviewed generally reflected appropriate standards, such as government-wide policy and guidance issued by the Office of Management and Budget, recommended security controls and practices contained in the National Institute of Standards and Technology's Special Publications, and requirements contained in federal statutes, such as the Privacy Act of 1974 and the Federal Information Security Modernization Act of 2014. The report also notes, however, that recent audits of the FDIC's information security controls and practices, some of which pertain to covered systems, found that although the FDIC generally had system access controls in place, appropriate standards had not always been followed as evidenced by the findings and recommended control improvements identified during the audits.

Consistent with the audit's objective, C&C's report does not contain recommendations.

Corporation Comments

Subsequent to the issuance of C&C's draft report, representatives of the FDIC's Chief Information Officer (CIO) Organization and the Division of Information Technology (DIT) provided additional information for C&C's consideration, and the firm clarified its report to reflect this information, as appropriate. Because the report contains no recommendations, the CIO and Director, DIT, elected not to provide a written response.

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

Office of Audits and Evaluations
Office of Inspector General

DATE: August 11, 2016

MEMORANDUM TO: Lawrence Gross, Jr.
Chief Information Officer

Russell G. Pittman, Director
Division of Information Technology

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

SUBJECT: *The Cybersecurity Act of 2015—The FDIC's Controls and Practices Related to Covered Systems* (Report No. AUD-16-005)

The subject final report is provided for your information and use. Please refer to the Executive Summary, included in the report, for the overall audit results.

The report did not contain recommendations, thus a written response was not required. As required by the Cybersecurity Act of 2015, we are providing a copy of this report to the appropriate committees of jurisdiction in the United States Senate and the House of Representatives.

If you have any questions concerning the report, please contact me at (703) 562-6316 or Joseph E. Nelson, Information Technology Audit Manager, at (703) 562-6314. We appreciate the courtesies extended to the Office of Inspector General and contractor staff during the audit.

Attachment

THE CYBERSECURITY ACT OF 2015 – THE FEDERAL DEPOSIT INSURANCE CORPORATION'S CONTROLS AND PRACTICES RELATED TO COVERED SYSTEMS

AUGUST 11, 2016

Cotton & Company
Answers Questioned

Cotton & Company LLP
635 Slaters Lane
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
lschwartz@cottoncpa.com | www.cottoncpa.com

TABLE OF CONTENTS

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

August 11, 2016

Mark F. Mulholland
Assistant Inspector General for Audits
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: The Cybersecurity Act of 2015 – The FDIC's Controls and Practices Related to Covered Systems

Cotton & Company LLP is pleased to submit this report in support of the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) reporting responsibilities pursuant to Section 406 of the Cybersecurity Act of 2015. The FDIC OIG engaged Cotton & Company LLP to conduct this performance audit pursuant to contract number CORHQ-15-G-0161. Cotton & Company performed the work from April through August 2016.

The objective of our audit was to describe the FDIC's information security policies, procedures, practices, and capabilities for covered systems as prescribed by Section 406 of the Cybersecurity Act of 2015. Consistent with the provisions of the statute, we generally did not assess the adequacy of the FDIC's information security controls over the covered systems. Except as noted in the report, our results are as of May 4, 2016. We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,
Cotton & Company LLP

Loren Schwartz, CPA, CISSP, CISA
Partner, Information Assurance

INTRODUCTION

On December 18, 2015, the Consolidated Appropriations Act, 2016 (Public Law (P.L.) 114-113), was enacted into law. P.L. 114-113 Division N, Cybersecurity Act of 2015, Title IV, *Other Cyber Matters*, Section 406, *Federal Computer Security,* (referred to herein as the Cybersecurity Act) requires the Inspector General of each covered agency (as described in Section 406), including the FDIC, to submit to the appropriate committees of jurisdiction in the United States Senate and House of Representatives a report which is to contain information collected from the covered agency on various computer-security-related topics regarding the "Federal computer systems"[1] used by the agency. This report fulfills that statutory requirement. As prescribed in the Cybersecurity Act, this report includes descriptions of:

(A) The logical access policies and practices that the FDIC uses to access a covered system (described in Section 406 as a national security system as defined in Section 11103 of Title 40, United States Code (U.S.C.), or a federal computer system that provides access to personally identifiable information (PII)), including whether the FDIC followed appropriate standards.

(B) The logical access controls and multi-factor authentication (MFA) that the FDIC uses to govern access to covered systems by privileged users.

(C) The reasons why the FDIC does not use logical access controls or MFA (in the event that the FDIC does not use one or both).

(D) The following information security management practices that the FDIC uses with regard to covered systems:

i. Policies and procedures followed to conduct inventories of software present on covered systems, and licenses associated with such software.

ii. The capabilities used by the FDIC with regard to monitoring and detecting exfiltration and other threats, including:

(I) Data loss prevention (DLP)

(II) Forensics and visibility

(III) Digital rights management (DRM)

iii. How the FDIC is using the capabilities referenced in (ii) above.

iv. The reasons for not using the capabilities described in (ii) above (in the event that the FDIC is not utilizing those capabilities).

(E) The FDIC's policies and procedures for ensuring that entities, including contractors, that provide services to the FDIC are implementing the information security management practices described above in (D).

OBJECTIVE

The objective of this audit was to describe the FDIC's information security policies, procedures, practices, and capabilities for covered systems as prescribed by Section 406 of the Cybersecurity Act of 2015. In accordance with the statute, we generally did not assess the adequacy of the FDIC's information security controls over the covered systems.

[1] Terms that are underlined when first used in this report are defined in Appendix II – Glossary.

SCOPE AND METHODOLOGY

The scope of this performance audit was limited to describing the information security policies, procedures, practices, and capabilities for covered systems as prescribed by Section 406 of the Cybersecurity Act. FDIC officials provided Cotton & Company LLP with a list of covered systems as defined by the statute that were in use as of May 4, 2016. The primary source of this list was an existing inventory of FDIC-owned systems and systems operated on behalf of the FDIC that contained PII. Cotton & Company LLP performed audit procedures to ensure that the FDIC's list was reasonably complete for purposes of conducting the audit. As part of that work, we identified one additional covered system that we included in the scope of the audit.

To determine whether the FDIC followed appropriate standards, and in order to develop descriptions of the FDIC's information security policies, procedures, practices, and capabilities for covered systems, we interviewed FDIC personnel familiar with relevant controls and practices; reviewed corroborating documentation, such as policies, procedures, and relevant criteria; and evaluated the results of other audits. We have included these descriptions in the Results section below. Except as noted in this report, our results are as of May 4, 2016.

Cotton & Company LLP conducted the audit onsite at the FDIC's Virginia Square location in Arlington, Virginia, from April through August 2016 in accordance with Generally Accepted Government Auditing Standards.

BACKGROUND

The FDIC is a government corporation and as such, laws, regulations, and standards governing information security controls and practices that apply to other federal agencies do not always apply to the FDIC. However, certain federal statutes, such as the Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act of 2014 (FISMA), define "agency" as including government corporations and independent regulatory agencies and, therefore, these statutes apply to the FDIC. The Federal Deposit Insurance Act (12 U.S.C. 1811 et seq.) generally grants the FDIC a degree of independence from direct oversight by the Office of Management and Budget (OMB). However, the FDIC evaluates individual policies and guidance issued by OMB to determine the extent to which they may apply to the FDIC.

The FDIC's Board of Directors has responsibility for the security of the FDIC's information and information systems. FDIC division and office heads also play an important role in information security. These individuals are responsible for ensuring that information systems under their ownership or control conform to the FDIC's information security program requirements. Further, the FDIC's Chief Information Officer (CIO), who reports directly to the FDIC Chairman, has broad strategic responsibility for information technology (IT) governance, investments, program management, and information security. The FDIC's Chief Information Security Officer (CISO), who reports directly to the CIO, is responsible for carrying out the CIO's responsibilities under FISMA—most notably, to plan, develop, and implement an agency-wide information security program. The CIO and CISO coordinate closely with the Director, Division of Information Technology (DIT), who is responsible for managing the FDIC's IT functions. The Director, DIT, reports to the CIO.

Information security managers (ISMs) located within the divisions and offices provide a business focus on information security and coordinate with the CIO organization to ensure that appropriate security controls are in place to protect their respective division's or office's information and information systems. ISMs are responsible for educating employees and contractors regarding methods for properly safeguarding FDIC information; assessing system security levels; ensuring that the FDIC addresses security requirements in new and enhanced systems; and promoting compliance with security policies and procedures. Internal control liaisons within the divisions and offices work with the ISMs to identify and ensure the implementation of appropriate security controls within business processes.

The Division of Administration's Security and Emergency Preparedness Section is responsible for administering the FDIC's physical and personnel security programs, which are fundamental components of the overall information security program. Physical security includes such activities as badging employees, contractors, and visitors and protecting employees, visitors, and facilities from internal and external threats, such as fire, theft, vandalism, sabotage, and terrorist activities. Personnel security includes activities such as performing background investigations and credit checks of FDIC employees and contractor personnel to ensure that the FDIC employs and retains only those persons who meet federal requirements for suitability and whose conduct would not jeopardize the accomplishment of the FDIC's duties or responsibilities.

RESULTS

The FDIC has 269 systems that meet the Cybersecurity Act's definition of a covered system. The 269 systems can be divided into three groups as follows:

- 166 FDIC-owned systems.
- 11 contractor systems, also known at FDIC as outsourced provider *systems*.
- 92 contractor services, also known at FDIC as outsourced provider *services*.

Below are descriptions of the FDIC's information security policies, procedures, practices, and capabilities applicable to each of the above referenced groups of systems. The descriptions are organized by the Section 406 requirements described on page 2 of this report.

Cybersecurity Act Requirement A

> *A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.*

Description of Relevant FDIC Information Security Policies, Procedures, and Practices

The following FDIC policy directives apply to logical access for the 166 FDIC-owned systems and for the 11 outsourced provider *systems*:

- FDIC Circular 1360.15*, Access Control for Information Technology Resources*, dated March 2011, requires (among other things) that access be authorized based on business needs, consistent with the security principle of least-privilege, and (if warranted) through pre-defined roles. The Circular also contains provisions related to segregation of duties, and the timely removal, periodic monitoring, and review of access.
- FDIC Circular 1300.4, *Acceptable Use Policy for Information Technology Resources*, dated April 2016, provides policy on personal and prohibited uses of the Corporation's IT resources.

In support of Circular 1360.15, the FDIC defines various types of sensitive data that apply to a broad range of information that requires protection based on how the information is categorized and defined. Specifically,

- FDIC Circular 1360.9, *Protecting Sensitive Information*, dated October 2015, establishes FDIC policy on protecting sensitive information collected and maintained by the FDIC and provides guidance for safeguarding the information. The circular also defines the terms PII and sensitive information.
- FDIC Circular 1360.19, *Privacy Impact Assessment Requirements*, dated May 2012, establishes policy and provides guidance for identifying the sensitive information and levels of PII contained within a system or application, based on the impacts of (1) new or substantially changed IT developed or procured by FDIC that collects, maintains, or disseminates PII; (2) proposed rulemakings that impact the privacy of PII; and

(3) any other internal or external activity that involves the electronic collection and use of PII. The provisions in this circular apply to all FDIC employees and contractors involved in the development or implementation of IT, rulemakings, or other electronic collection activities subject to the E-Government Act of 2002 (Section 208) and the Consolidated Appropriations Act, 2005 (Section 522 of Division H).

The following FDIC policy directives apply to logical access for the 92 outsourced provider *services*:

- FDIC Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/Third Party Products*, dated February 2016, establishes a framework for incorporating security into all phases of the IT acquisition process, including the establishment of IT security requirements for third-party providers that wish to provide automated data processing contract services or products to the FDIC. This Circular applies to (1) all FDIC employees responsible for procuring and/or implementing information systems at the FDIC; (2) contractors and others who participate in IT contracting with the FDIC; and (3) non-FDIC products and individuals that service, handle, manage, or interface with FDIC data or information systems.
- FDIC Circular 3700.16, *Acquisition Policy Manual*, dated January 2015, and the accompanying *Acquisitions Procedures, Guidance and Information* (PGI) document, dated April 2016, identify the various contract clauses that apply to outsourced vendor (referred to herein as provider) *services* and establish the framework of requirements within the contract. The federal statutes, regulations, and executive orders described within the Acquisitions PGI document apply to the FDIC contracting program and must be considered in the acquisition planning process.

We noted that FDIC policies applicable to logical access for covered systems that we reviewed generally reflected appropriate standards, such as:

- Government-wide policy and guidance issued by the OMB, including OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (Transmittal Memorandum No. 4, dated November 28, 2000[2]), and applicable memoranda related to safeguarding PII;
- Recommended security controls and practices in the National Institute of Standards and Technology's (NIST) Special Publications (SP); and
- Requirements contained in federal statutes, such as the Privacy Act of 1974 and FISMA 2014.

Recent audits of the FDIC's information security controls and practices, some of which pertain to covered systems, found that although the FDIC generally had system access controls in place, appropriate standards had not always been followed as evidenced by the findings and recommended control improvements identified during the audits.[3]

Cybersecurity Act Requirement B

A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

[2] On July 28, 2016, OMB published a revision to Circular A-130 and its appendices. We did not review the revised Circular because we finished our fieldwork prior to the Circular's publication date.

[3] See GAO report, entitled *INFORMATION SECURITY FDIC Implemented Controls over Financial Systems, but Further Improvements Are Needed*, (Report No. GAO-16-605, dated June 2016) at http://www.gao.gov/assets/680/678084.pdf, and FDIC OIG Executive Summary, entitled *Audit of the FDIC's Information Security Program—2015* (Report No. AUD-16-001, dated October 2015) at https://fdicig.gov/reports16/16-001AUD.pdf.

Description of Relevant FDIC Information Security Policies, Procedures, and Practices

The following information applies to the 166 FDIC-owned systems.

In addition to the FDIC Circulars addressing access controls referenced in the Cybersecurity Act Requirement A section of this report, DIT has established the following policies that define requirements and guidance regarding logical access for privileged users:

- 16-002 – *Policy on Administrator Account Naming and Password Length,* dated March 18, 2016, which requires, among other things, the use of specialized User IDs and enhanced password requirements for privileged users.
- 14-005 – *Policy on Restricting Administrative Access to both Servers and Workstations,* dated July 1, 2014, which restricts accounts with administrative privileges to authenticating to only one type of computing platform (i.e., servers or workstations).
- 12-008 – *Policy on Restricting Administrative Access to User E-mail and Mailboxes,* dated June 30, 2013, which provides guidance to DIT contractors and employees regarding the circumstances in which mailboxes may be accessed using administrative-type accounts.

The FDIC has drafted, but not yet finalized, a corporate policy requiring privileged users to use MFA when accessing the FDIC's IT network (which, in turn, provides access to covered systems). In practice, however, privileged users have used a token-based MFA solution to access the IT network since 2014. In addition, privileged users are required to use MFA when accessing the IT network remotely.

The following information applies to the 11 outsourced provider *systems* and the 92 outsourced provider *services*.

The FDIC has developed standard security clauses that are required to be included in both new IT contracts and existing contracts that are renewed for outsourced provider *systems* and *services*. In general, the clauses require the providers to implement adequate administrative, technical, physical, and procedural security controls to ensure that FDIC information in the providers' possession or under the providers' control is adequately protected from loss, misuse, and unauthorized access or modification. The clauses also require compliance with certain federal laws and standards addressing information security and privacy including, for example, NIST SPs and the Privacy Act of 1974, as well as FDIC security policies, such as FDIC Circular 1360.9, *Protecting Sensitive Information*. The clauses do not, however, specifically address MFA for privileged users. As a result, outsourced providers are not explicitly required to implement MFA for privileged users.

Information regarding the use of MFA by the FDIC's outsourced provider *systems* and *services* was not readily available. However, an official in the CIO Organization informed us that outsourced provider *systems* and *services* generally do not require MFA for privileged user access. The official added that requiring the use of MFA across the FDIC's portfolio of outsourced providers poses practical challenges. For example, vendors would likely use a variety of MFA solutions that the FDIC would need to use and assess.

Cybersecurity Act Requirement C

> *If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.*

Description of the Reasons for Not Always Using Multi-Factor Authentication to Access Covered Systems

The following information applies to the 166 FDIC-owned systems.

Both privileged and non-privileged users are required to use MFA when accessing the FDIC's IT network remotely. In addition, privileged users use a token-based MFA solution when accessing the IT network from within FDIC facilities. However, non-privileged users do not use MFA to access the IT network from within FDIC facilities.

In September 2015, the FDIC made a decision to implement a token-based MFA solution for non-privileged users accessing the IT network from FDIC facilities. In early 2016, the FDIC shifted direction on this effort and decided to instead implement a Personal Identity Verification (PIV) card-based MFA solution for both privileged and non-privileged IT network users. This change in direction was prompted by the issuance of OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, dated October 30, 2015, which directed federal agencies to issue and use PIV cards for MFA. At the close of our audit, the FDIC was working to issue PIV cards to its employees and contractors to enable the use of the new MFA solution. The FDIC plans to begin enforcing the use of PIV cards to authenticate to the IT network in 2017.

The following information applies to the 11 outsourced provider *systems* and the 92 outsourced provider *services*.

An official in the CIO Organization informed us that the reasons why MFA may or may not be used for each of the FDIC's outsourced provider *systems* were not readily available. However, as noted earlier in this section, MFA is not always used to access FDIC systems. The official added that the FDIC's outsourced provider *services* are generally not considered to be federal systems and, therefore, may not be required to use MFA. The FDIC requires that its IT contracts for outsourced provider *systems* and *services* contain clauses that are intended to help ensure providers follow the FDIC's security policy requirements. Concepts and principles in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, have been incorporated into standard clauses that are included in both new IT contracts and existing contracts that are renewed. However, these clauses do not specify the technologies that must be used to meet the FDIC's security policy requirements. As a result, the contracts do not require outsourced provider *systems* and *services* to use MFA.

Cybersecurity Act, Requirement D, Part (i)

> *(D) A description of the following information security management practices used by the covered agency regarding covered systems:*
>
> > *(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.*

Description of Relevant FDIC Information Security Policies and Procedures

The following information applies to the 166 FDIC-owned systems. The 11 outsourced provider *systems* and 92 outsourced provider *services* are covered under Requirement E.

FDIC Circular 1380.2, *FDIC Information Technology Asset Management Life Cycle Program*, states that DIT must conduct an annual software asset inventory to ensure that the FDIC is in compliance with software licensing requirements. The FDIC also has an Infrastructure Support Contract (ISC 3) which states, "The contractor shall conduct a quarterly inventory of all hardware and software assets that are not under maintenance agreements and shall report each asset that is not under a maintenance agreement and rationale." The ISC 3 includes requirements for information that the contractor needs to report in the software inventory. However, the ISC 3 contractor has not yet fully developed standard operating procedures for conducting inventories of the software present on covered systems and the licenses associated with the software. A DIT official informed us that the ISC 3 contractor was working to develop such procedures.

Cybersecurity Act, Requirement D, Parts (ii) through (iv)

> *(D) A description of the following information security management practices used by the covered agency regarding covered systems:*
>
> *…*
>
> *(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –*
>
> *(I) data loss prevention capabilities;*
>
> *(II) forensics and visibility capabilities; or*
>
> *(III) digital rights management capabilities*
>
> *(iii) A description of how the covered agency is using the capabilities described in clause (ii).*
>
> *(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.*

Description of Relevant FDIC Information Security Practices and Capabilities

The following information applies to the 166 FDIC-owned systems. The 11 outsourced provider *systems* and 92 outsourced provider *services* are covered under Requirement E.

Data Loss Prevention: The FDIC has implemented a commercially available DLP solution to help ensure that sensitive FDIC data are secured consistent with policy. The FDIC's Information Security and Privacy Staff (ISPS) manage the DLP tool, which uses keywords and pattern searches based on pre-defined rule sets to monitor and inspect FDIC data in three different states:

1) Data at rest (e.g., inactive data, such as fileshares on the internal FDIC IT network);

2) Data in motion (e.g., data in the process of being transmitted through email or web uploads); and

3) Data at endpoints (e.g., data in end-user devices, such as workstations/desktops, laptops, removable media, or print jobs).

The DLP tool has additional preventative blocking capabilities based on the volume of data/records or specific events being transmitted and the FDIC user's role and function.

Forensics and Visibility: The FDIC has established a forensics team within ISPS to conduct forensics analysis into IT matters that require investigations. The FDIC forensics team's capabilities include such things as:

- Obtaining open-source intelligence and maintaining paid subscriptions for intelligence related to threat vectors as they arise.
- Obtaining notifications from the FDIC's case ticketing system regarding events of interest on the FDIC's IT network.
- Maintaining forensic activity logs for 3 years.

The forensics team uses a variety of software tools to support such things as:

- Password cracking, penetration testing, reverse-engineering, network logging and tracking, packet analysis, and software program whitelisting.
- Analysis on and off the FDIC's IT network (e.g., forensic analysis of cell phones; monitoring of public internet sites for potential fraud involving the FDIC; log, disk, and memory analysis; and honeypot workstation monitoring).

- Public records research, the extraction of FDIC emails related to security incidents, and employee investigations.

In addition, the FDIC has implemented a Security Information and Event Management (SIEM) tool to enable visibility across the IT network. The SIEM tool serves as a network log aggregator and is able to search logs related to multiple network devices, including firewalls, servers, the Intrusion Detection System (IDS), and endpoint systems. The FDIC also uses software tools for capturing security events across its IT network.

Digital Rights Management: The FDIC defines DRM, or Information Rights Management (IRM), as various technical controls designed to provide persistent protection to documents to prevent them from being printed, forwarded, or copied by authorized users, or accessed or viewed by unauthorized users. The FDIC has not adopted DRM technology. However, in 2013, the FDIC analyzed the potential application of DRM to certain business processes. In performing the analysis, the FDIC gathered high-level business requirements, investigated DRM capabilities, and conducted market research of potential solutions. A CIOO official involved at the time informed us that there were better controls, such as DLP, to pursue from a cost-benefit perspective than DRM. The official added that the FDIC discussed DRM technology at the time with independent IT research firms and discovered it was not a widely implemented technology owing both to the complexity of the software implementation and maintenance, and its relative immaturity as an enterprise product. At the close of our audit, the FDIC was actively researching, evaluating, and testing commercially available DRM solutions and planned to implement such a solution in the future.

Cybersecurity Act Requirement E

> *A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).*

Description of Relevant FDIC Information Security Policies, Procedures, and Practices

With respect to the information security practices described in subparagraph (D) of the Cybersecurity Act**,** the following information applies to the 11 outsourced provider *systems* and 92 outsourced provider *services*.

The clauses included in outsourced provider contracts do not specifically require providers to conduct inventories of software present on outsourced provider *systems* and *services* used by the FDIC and licenses associated with such software. However, contract awards valued over $100,000 are required to include the following clause, "Contractor will have in its possession all necessary licenses, permits and approvals required to execute, deliver and perform its duties under this contract no later than ten (10) days after the execution of the contract."

As described earlier in this report, the FDIC has developed standard security clauses that, as a matter of practice, are included in contracts for outsourced provider *systems* and *services*. The clauses do not, however, specifically require outsourced providers to utilize capabilities for DLP, forensics and visibility, or DRM to monitor and detect exfiltration and other threats, nor was information readily available regarding the extent to which the FDIC's outsourced providers used such capabilities.

More broadly, the Acquisitions PGI document requires that IT contracts contain the following clauses that are intended to help ensure contractors follow the FDIC's security policy requirements. Concepts and principles in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, have been incorporated into these clauses, which are included in both new IT contracts and existing contracts that are renewed:

- 7.4.2-1 Security and Privacy Compliance for IT Services – to be inserted in all awards for services in which the contractor (interchangeably referred to as vendor) or its subcontractors may develop or maintain IT applications or implement or operate other IT resources.
- 7.4.2-2 Off-site Processing and Storing of FDIC Information – to be inserted in all awards in which FDIC information (electronic or paper form) may be processed or stored offsite in a non-FDIC facility.
- 7.4.2-3 Data Connection – to be inserted in all awards in which a data connection may be established between the FDIC IT network and the contractor located at a non-FDIC facility.
- 7.4.2-4 Privacy Requirements for External Web Applications and Content – to be inserted in all awards in which the contractor may develop or maintain applications or content located on an FDIC-website accessed by the public.
- 7.5.1-1 Privacy Act – to be inserted in all awards that require the design, development, or operation of a system of record(s) on individuals.
- 7.5.1-2 Protecting Sensitive Information – to be inserted in all awards in which the contractor, its personnel, or its subcontractors may have access to FDIC facilities or systems, or otherwise may have access to FDIC sensitive information.
- 7.5.1-3 Access to FDIC Information Systems – to be inserted in awards for services in which contractor personnel or subcontractor personnel may have access to the FDIC's IT network and/or information systems.

The following FDIC security policies are referenced in the above contract clauses:

- FDIC Circular 1360.17, *FDIC Information Technology Security Guidance for FDIC Procurements/Third Party Products* (described earlier).
- FDIC Circular 1360.16, *Mandatory Information Security Awareness Training*, dated July 2002, mandates annual information security awareness training for all employees and contractors who are involved with the management, use, or operation of a Federal computer system within or under the supervision of the FDIC.
- FDIC Circular 1360.9, *Protecting Sensitive Information* (described earlier).
- FDIC Circular 1300.4, *Acceptable Use Policy for Information Technology Resources* (described earlier).
- FDIC Circular 1360.10, *Corporate Password Standards*, dated February 2003, states that it is the policy of the FDIC that access to all FDIC Automated Information Systems (AISs) containing or potentially containing sensitive data and for which user accountability is required shall be granted only through the use of a valid and current password.
- FDIC Circular 1360.15, *Access Control for Information Technology Resources* (described earlier).
- FDIC Circular 1360.12, *Reporting Computer Security Incidents*, dated June 2003, requires that all users of FDIC AISs report suspected computer security incidents affecting all FDIC AIS resources to the FDIC Computer Security Incident Response Team (CSIRT). FDIC CSIRT shall investigate and track all reported security incidents and report security incidents affecting general support systems and major applications to the CIO and FDIC management officials responsible for the security of FDIC AIS resources.

In addition, as part of the corporate-wide IT Security Risk Management Program, the FDIC has established an *Outsourced Information Service Provider Assessment Methodology* to address security risks associated with the FDIC's outsourced provider *services*. The Methodology requires the completion of security and privacy activities and, based on the risk, technical security assessments and site visits for outsourced provider *services*.

APPENDIX I – LIST OF ACRONYMS

Acronym	Description
AIS	Automated Information Systems
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DIT	Division of Information Technology
DLP	Data Loss Prevention
DRM	Digital Rights Management
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
IDS	Intrusion Detection System
IRM	Information Rights Management
ISC 3	Infrastructure Support Contract 3
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PGI	Procedures, Guidance and Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
SIEM	Security Information and Event Management
SP	Special Publication
U.S.C.	United States Code

APPENDIX II – GLOSSARY

Term	Definition
Appropriate Standards	For purposes of this audit, we defined appropriate standards as NIST SPs and legally applicable OMB policy and guidance that address access control requirements.
Computer Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
Data Loss Prevention	A strategy for making sure that end users do not send sensitive or critical information outside a corporate network. The term is also used to describe software products that help network administrators control what data end users can transfer. Adoption of DLP is being driven by insider threats and by more rigorous state privacy laws, many of which have stringent data protection or access components. In addition to being able to monitor and control endpoint activities, some DLP tools can also be used to filter data streams on the network and protect data in motion. DLP products may also be referred to as data leak prevention, information loss prevention or extrusion prevention products.
Digital Rights Management	Access control technologies that are used to restrict usage of proprietary hardware and copyrighted works. DRM technologies try to control the use, modification, and distribution of copyrighted works (such as software and multimedia content), as well as systems within devices that enforce these policies.
Federal Computer Systems	The term "Federal computer systems" is not defined in section 406, but for purposes of this audit, we interpreted that term to mean IT systems used or operated by, or on behalf of, the FDIC.
Forensics and Visibility	The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.
Logical Access Controls	Per Section 406 of the Cybersecurity Act, "logical access control" means a process for granting or denying specific requests to obtain and use information and related information processing services.
Multi-Factor Authentication	Per Section 406 of the Cybersecurity Act, "multi-factor authentication" means the use of not fewer than two authentication factors, such as the following:

Term	Definition
	(A) Something that is known to the user, such as a password or personal identification number. (B) An access device that is provided to the user, such as a cryptographic identification device or token. (C) A unique biometric characteristic of the user.
Outsourced (Information) Provider Service	According to the FDIC's *Outsourced Information Service Provider Assessment Methodology*, an outsourced (information) provider service is a specific third-party information processing solution procured with the intent of leveraging existing technologies and processes which provide significant cost reduction over an outsourced or agency owned information system. Any one of the following must be true about an outsourced information service: 1) The outsourced information service uses proprietary technology to provide the same solution to multiple clients and as a result only a fraction of the technology components may be available for the FDIC's review (e.g., Software as a Service, Cloud Computing, etc.). 2) The outsourced information service acts as a hosting provider for a Commercial Off The Shelf product whose application logic has not been altered. 3) The outsourced information service does not receive data feeds from the FDIC and all data feeds are from outsourcer to the FDIC. (This does not apply to user provided input or initial data-loads). 4) The outsourced information service provides only pay-per use Central Processing Unit cycles (e.g., grid computing, and symmetric multi-processing) without any application or transactional logic.
Outsourced (Information) Provider System	According to the FDIC's *Outsourced Information Service Provider Assessment Methodology*, an outsourced (information) provider system is a system or group of systems supporting the FDIC's mission which is operated by an independent third party and has any one of the following characteristics: 1) The FDIC has direct input into the systems development lifecycle of the system. 2) The system contains business or transactional logic which has been designed from the ground-up to meet specific needs of the FDIC.

Term	Definition
	3) The outsourced system is not shared by other organizations and at least 51% of system's operational costs are paid by the FDIC. 4) The outsourced information service provider has been contracted to host an FDIC designed system. 5) The system owner is another federal agency which is required to comply with FISMA. Based on the above definition of outsourced information systems, these systems operate under the same premise as wholly-owned FDIC information systems. It is assumed that outsourced information systems are designed primarily for the FDIC and typically their development lifecycle is at the discretion of the FDIC.
Personally Identifiable Information	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Privileged Users	Per Section 406 of the Cybersecurity Act, "privileged user" means "a user who has access to system control, monitoring, or administrative functions." The FDIC has established a definition of privileged users which we believe is consistent with the statutory definition, namely, those users who have administrative privileges to servers and workstations. This includes database administrators, server administrators, and desktop administrators. Accordingly, we employed the FDIC's definition for purposes of this audit.