Controls Over System Interconnections with Outside Organizations

December 2018 **AUD-19-002**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

Office of Inspector General

Executive Summary

Controls Over System Interconnections with Outside Organizations

The Federal Deposit Insurance Corporation (FDIC) exchanges significant amounts of data with outside organizations, including Federal agencies and non-governmental entities, through system interconnections. Such data includes personally identifiable information, confidential bank examination information, and sensitive financial data.

The National Institute of Standards and Technology (NIST) defines a system interconnection as a direct connection of two or more information technology systems for the purpose of sharing data and other information resources. NIST defines a life-cycle approach for managing and securing interconnected systems consisting of four phases: planning, establishing, maintaining, and terminating interconnections. According to NIST, if system interconnections are not designed properly, they can expose Federal agencies to security risks, such as unauthorized access or disclosure of agency information.

The objective of the audit was to assess the FDIC's controls for managing system interconnections with outside organizations. The audit focused on key controls recommended by NIST for managing system interconnections, such as written agreements that specify the technical and security safeguards needed to protect interconnections.

Results

Although the FDIC issued certain policies, procedures, and templates for establishing system interconnections, we identified control weaknesses in each of the four phases of the NIST life-cycle framework.

We found that the FDIC's policies and procedures did not define the types of technologies and configurations that constitute a system interconnection and, therefore, require a written agreement. In addition, the FDIC's policies and procedures did not articulate the roles and responsibilities for all stakeholders involved in managing system interconnections. Further, the FDIC did not establish documentation requirements for key activities.

The FDIC also did not create written agreements to govern several of its system interconnections. In some cases, the FDIC relied on language in its contracts with outside organizations to satisfy the intent of a written agreement. However, these contracts did not address all elements recommended by NIST for managing system

interconnections. In one instance, the FDIC could not provide any information about the interconnection, including the date it was established, the type of data exchanged, the security controls employed, or who approved the interconnection.

Further, we identified instances in which written agreements governing system interconnections had expired, even though the underlying connections remained enabled. In addition, many of the written agreements we reviewed did not contain current information for senior FDIC officials responsible for the interconnection to operate. Finally, the FDIC did not always terminate system interconnections when they were no longer needed, nor did the FDIC establish a process for notifying outside organizations of its intent to terminate system interconnections. In light of these control weaknesses, the FDIC could not be assured that its system interconnections were properly managed or secured to protect sensitive information from unauthorized access or disclosure.

We identified an additional matter involving the need for policies and procedures to govern the secure transfer of data outside of the FDIC using technologies that do not constitute system interconnections.

Recommendations

We recommended that the CIO (1) modify existing policies and procedures to address all four phases of the NIST life-cycle framework for managing system interconnections; (2) execute written agreements with two outside organizations; (3) modify the FDIC's standard contract language involving system interconnections to align with NIST guidance; (4) review system interconnection agreements annually to ensure they remain current; (5) implement procedures to review, update, and reauthorize written agreements when appropriate; (6) develop and implement procedures for notifying technical staff when system interconnections are terminated; and (7) develop and implement policies and procedures to govern the secure transfer of data outside the FDIC when using technologies that are not considered system interconnections.

In a written response to the report, the CIO Organization concurred with six of the report's recommendations and partially concurred with the remaining recommendation. The CIO Organization provided an alternative corrective action to address the remaining recommendation. The CIO Organization expects to complete actions to address all of the recommendations by September 30, 2019.

Contents

Background **2**

The FDIC's System Interconnections 5
Roles and Responsibilities 6

Audit Results **7**

FDIC Lacking Complete Policies and Procedures 8
Agreements for Certain Interconnections Not Established 11
Expired FDIC Agreements Governing Interconnections 14
FDIC Interconnections Remained Enabled When No Longer Justified 16
Secure File Transfers and Secure Sockets Layer VPNs 18

FDIC Comments and OIG Evaluation **20**

Appendices

1. Objective, Scope, Methodology 21
2. Glossary 24
3. Acronyms and Abbreviations 26
4. Corporation Comments 27
5. Summary of the Corporation's Corrective Actions 32

Tables

1. Inventory of System Interconnections 5
2. System Interconnections With/Without MOAs and ISAs 12
3. System Interconnections with Expired ISAs and/or MOAs 14

Figures

1. Components of a System Interconnection 2
2. Life-Cycle Framework for Managing and Securing System Interconnections 3
3. Stakeholders Responsible for Managing System Interconnections 6

December 4, 2018

Howard G. Whyte, Chief Information Officer and Chief Privacy Officer
Chief Information Officer Organization

Subject | ***Controls Over System Interconnections with Outside Organizations***

The Federal Deposit Insurance Corporation (FDIC) exchanges significant amounts of data with outside organizations including Federal agencies and non-governmental entities through system interconnections. Such data includes personally identifiable information[1] (PII), including names, Social Security Numbers, and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers. The National Institute of Standards and Technology (NIST) defines a system interconnection as a direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources.[2] According to NIST, if system interconnections are not designed properly, they can expose Federal agencies to security risks, such as unauthorized access or disclosure of agency information. NIST recommends that agencies establish appropriate controls over system interconnections, such as written agreements that specify the technical and security safeguards needed to protect the interconnection.

Based upon a request from the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs, dated June 28, 2016, the Office of Inspector General (OIG) decided to review the system interconnections maintained by the FDIC and its management practices. The audit objective was to assess the FDIC's controls for managing system interconnections with outside organizations.

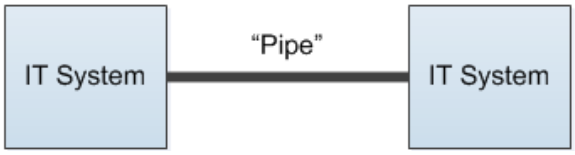
We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report contains our objective, scope, and methodology; Appendix 2 contains a glossary of terms; Appendix 3 contains a list of acronyms and abbreviations; Appendix 4 contains the FDIC's comments; and Appendix 5 contains a summary of the FDIC's corrective actions.

[1] Appendix 2, *Glossary*, defines terms that are underlined when first used in this report.
[2] NIST Special Publication (SP) *Security Guide for Interconnecting Information Technology Systems* (NIST Guide SP 800-47), August 2002.

BACKGROUND

In August 2002, NIST issued Guide SP 800-47 to provide Federal organizations with guidance for planning, establishing, maintaining, and terminating system interconnections.[3] According to NIST Guide SP 800-47, a system interconnection consists of three basic components: two IT systems and the mechanism by which the organizations connect the systems. NIST refers to the mechanism that connects the systems as a "pipe" through which data is made available, exchanged, or passed one-way only. Figure 1 illustrates the basic components of a system interconnection.

Figure 1: Components of a System Interconnection



Source: NIST Guide SP 800-47.

NIST Guide SP 800-47 explains that organizations might interconnect systems to exchange data and information among selected users, provide customized access to proprietary databases, collaborate on projects, and provide secure storage of critical data. NIST Guide SP 800-47 acknowledges that there are benefits associated with system interconnections, such as reduced operating costs, greater functionality, improved efficiency, and centralized access to data. For example, organizations can leverage other organizations' data and information rather than duplicating efforts. System interconnections can also strengthen relationships among organizations by promoting communication and cooperation.

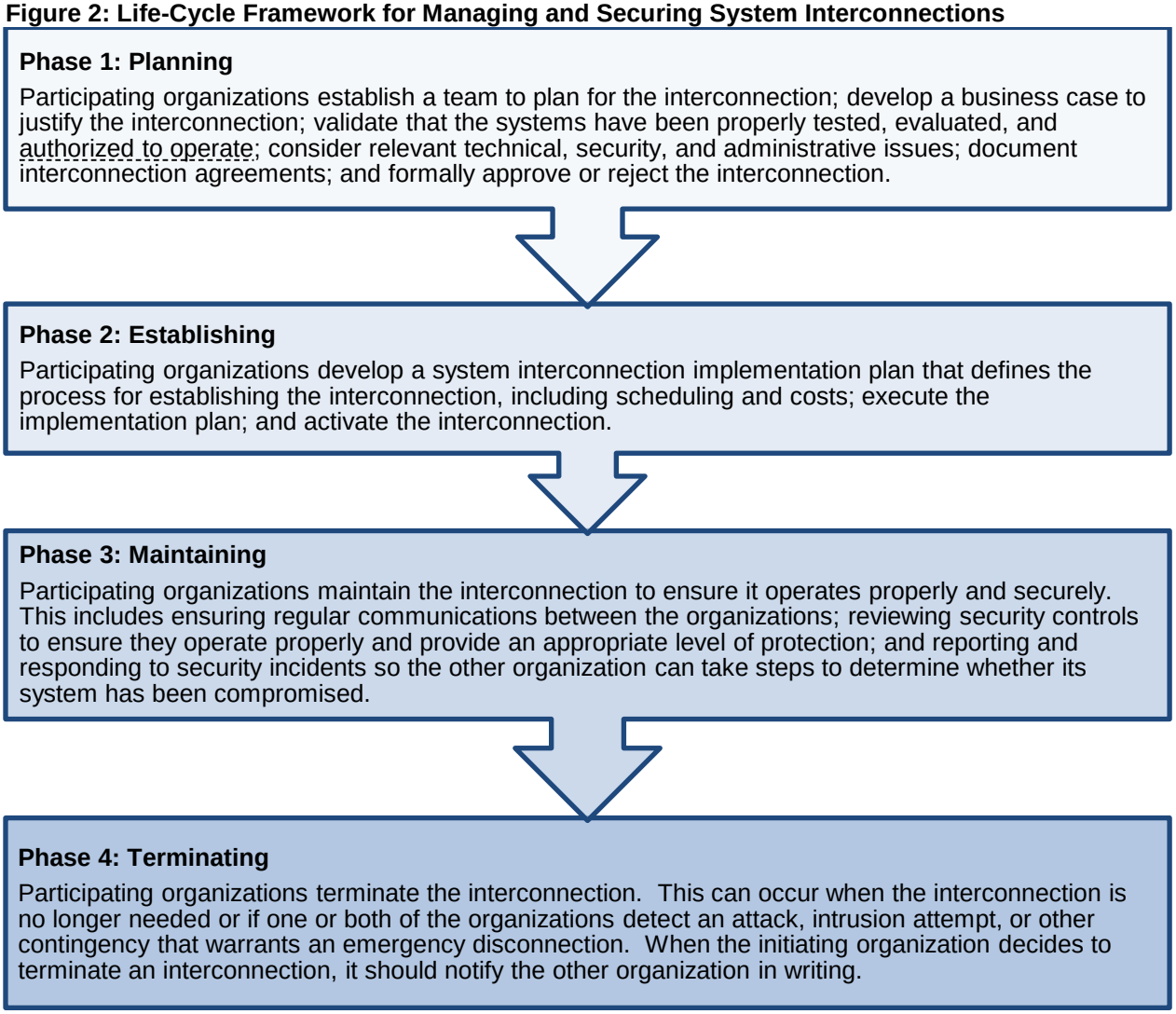
Notwithstanding these advantages, participating organizations must consider the risks that are introduced when they interconnect their systems and determine the appropriate controls needed to mitigate those risks. For example, NIST Guide SP 800-47 states that if the organizations do not properly design their system interconnections, security controls could fail, thus compromising the connected systems and providing unauthorized access to the data they store, process, or transmit. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data. Such a compromise at the FDIC could damage its network subjecting individuals to financial harm, such as identity theft or consumer fraud, and expose the FDIC to other liability and risks. NIST Guide SP 800-47 adds that because participating organizations have little or no control over the operation and

[3] NIST Guide SP 800-47 contains guidelines for use by Federal organizations consistent with Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource* (OMB A-130), July 2016. The FDIC has determined that OMB A-130 is generally legally applicable to the FDIC, subject to various caveats. One such caveat is that the FDIC should determine whether OMB instructions conflict with the FDIC's independence or regulatory authority.

management of the other organization's IT system, the risk of such compromise to an organization rises.

NIST Guide SP 800-47 defines a life-cycle approach for managing and securing interconnected IT systems. Figure 2 summarizes the four life-cycle phases which include planning, establishing, maintaining, and terminating.[4]

Figure 2: Life-Cycle Framework for Managing and Securing System Interconnections



Source: NIST Guide SP 800-47.

According to NIST Guide SP 800-47, organizations can use a dedicated line to connect their IT systems. A dedicated line is a leased or owned transmission line providing a constant transmission between two points. Dedicated lines provide a high level of security for interconnected systems because the lines can only be

[4] NIST Guide SP 800-47 uses the term terminating and disconnecting interchangeability when indicating a system interconnection is no longer needed.

breached through a direct physical intrusion. However, according to NIST, dedicated telecommunication lines can be expensive.

NIST Guide SP 800-47 states that one alternative for connecting systems is a virtual private network (VPN). A VPN is a data network that enables two or more parties to communicate securely over a network, such as the Internet, by creating a private connection. Because VPNs rely on a public network to transmit data, they require additional security measures, such as authentication and encryption, to ensure the confidentiality and integrity of the data. A VPN that is not properly encrypted and authenticated is less secure since an organization is transmitting data over the public Internet and an unauthorized party may be able to intercept the data. Conversely, a dedicated line can only be breached through direct physical intrusion. In addition, unlike dedicated lines, VPNs encrypt transmitted data and tend to be less costly to organizations. VPNs also provide organizations with flexibility because they do not need to purchase or lease dedicated lines to enable a connection.

According to NIST Guide SP 800-47, participating organizations in a system interconnection must establish written agreements that define how each organization will manage, operate, and use the interconnection. These agreements should also identify all relevant technical, security, and administrative issues surrounding the proposed interconnection in the form of a Memorandum of Agreement (MOA) and an Interconnection Security Agreement (ISA), or equivalent documents.

- According to NIST Guide SP 800-47, MOAs should document the relationship of the participating organizations in interconnecting two IT systems. The MOA serves as the authorization for the organizations to perform detailed planning for the interconnection that will ultimately lead to an ISA. The MOA defines the purpose of the system interconnection; identifies relevant authorities; specifies the responsibilities of each participating organization in establishing, operating, and securing the interconnection; and defines the terms of agreement, including the apportionment of costs between the participating organizations and the timeline for terminating or reauthorizing the system interconnection.

- According to NIST Guide SP 800-47, ISAs should contain detailed technical and security requirements for establishing, operating, and maintaining the system interconnection. The ISA documents the requirements for connecting the IT systems; describes the security controls an organization will use to protect the systems and data; and contains a technical drawing of the interconnection. The ISA addresses such things as the type of data the organizations will share; the manner in which the organizations will exchange the data; the required security configurations; and the manner in which the organizations will handle and report security incidents.

- An equivalent document can consist of a formal contract that incorporates all relevant technical, security, and administrative information. The NIST Guide SP 800-47 adds that organizations may use a formal contract especially if the interconnection is between a Federal agency and commercial organization.

The FDIC's System Interconnections

As of September 7, 2017, the FDIC had 11 system interconnections, as described in Table 1. These interconnections consisted of 10 VPNs[5] and *Connect: Direct*. *Connect: Direct* is file management software that FDIC uses to exchange data with other Federal agencies. The Chief Information Officer (CIO) Organization stated that it did not have any dedicated lines with outside organizations at the time of our fieldwork.

Table 1: Inventory of System Interconnections

Outside Organization	FDIC Business Use	Type of Connection
Organization 1	Host the FDIC's internal Website	VPN
Organization 2	Store FDIC legal records	VPN
Organization 3	Track security weaknesses related to IT systems	VPN
Organization 4	Support asset servicing functions for failed financial institutions	VPN
Organization 5	Process checks, credit card transactions, and electronic funds transfers	VPN
Organization 6	Process payroll for FDIC employees	VPN
Organization 7	Host the FDIC's internal training system	VPN
Organization 8	[The CIO Organization could not provide information about this connection]	VPN
Organization 9	Process purchase card payments	VPN
Organization 10	Submit and track Equal Employment Opportunity complaints	VPN
Organization 11	Exchange financial and supervisory data among financial regulatory agencies	Connect: Direct

Source: OIG analysis of the FDIC's network firewall rules[6] as of September 7, 2017.

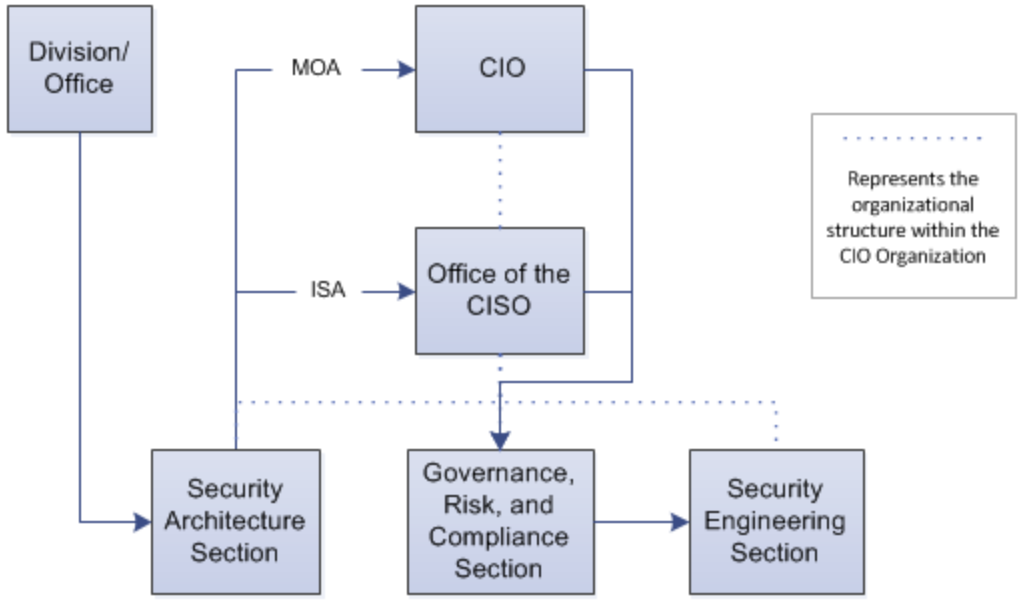
[5] The FDIC CIO Organization considers a VPN between systems that are configured as an Internet Protocol Security (IPsec) VPN to be a system interconnection. According to NIST SP *Guide to IPsec VPNs* (NIST Guide SP 800-77), December 2005, IPsec is a framework of open standards used to secure private communications over public networks. For example, the framework allows for secure communication between two networks, such as an organization's main office and a branch office, or two business partners' networks.

[6] The FDIC uses firewalls to control the flow of information into and out of its network. At the core of these firewalls is a set of customized instructions called rules that define permissible network traffic. The FDIC established firewall rules to permit the flow of data between interconnected systems.

Roles and Responsibilities

The CIO Organization has overall responsibility for managing the FDIC's system interconnections. The Office of the Chief Information Security Officer (CISO), a component within the CIO Organization, works with the FDIC's Divisions and Offices to plan, establish, maintain, and terminate system interconnections. Figure 3 depicts the key stakeholders involved in managing system interconnections along with a brief description of their roles and responsibilities.

Figure 3: Stakeholders Responsible for Managing System Interconnections



Source: OIG Analysis of the FDIC's MOA and ISA process and interviews of CIO Organization staff.

Divisions and Offices identify a business need for a system interconnection and draft the MOA and ISA. Once the CIO Organization establishes a system interconnection, information security managers (ISMs) within FDIC's Divisions and Offices are responsible for conducting annual reviews to ensure that MOAs and ISAs remain current.

Security Architecture Section within the Office of the CISO receives the draft MOA and ISA, and reviews each agreement for completeness. Once the review is complete, the Security Architecture Section routes the MOA and ISA to the CIO and CISO for review and signature.

CIO reviews the MOA to determine whether the risks associated with the interconnection are acceptable. If the CIO approves of the interconnection, the CIO signs the MOA.

Office of the CISO reviews the ISA to determine whether the agreement adequately addresses the technical configurations and security requirements of the system interconnection. If the CISO approves of the security requirements associated with the interconnection, the CISO signs the ISA.

Governance, Risk, and Compliance Section within the Office of the CISO receives and reviews the approved MOA and ISA to ensure the documents are complete and consistent with the Division or Office's request. Once reviewed, the Governance, Risk, and Compliance Section transmits its approval to the Security Engineering Section in order to establish the system interconnection.

Security Engineering Section within the Office of the CISO establishes the approved system interconnection and notifies the respective parties. The Security Engineering Section is also responsible for terminating system interconnections when they are no longer needed.

AUDIT RESULTS

Although the FDIC issued certain policies, procedures, and templates for establishing system interconnections, we identified control weaknesses in the four phases of the NIST life-cycle framework. Specifically, the FDIC did not:

- Establish policies and procedures to address key aspects of managing system interconnections;
- Create MOAs, ISAs, or contractual agreements to govern some system interconnections;
- Maintain current MOAs and ISAs for some interconnections; or
- Terminate system interconnections when no longer needed.

In light of these control weaknesses, the FDIC could not be assured that its system interconnections were properly managed nor secured to protect sensitive information from unauthorized access or disclosure.

We also noted that the FDIC should establish policies and procedures to govern the secure transfer of data outside of the FDIC using technologies for data exchange that do not meet NIST's definition of a system interconnection.

FDIC Lacking Complete Policies and Procedures

On March 9, 2006, NIST issued its Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. This FIPS 200 document states that policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government.[7] In addition, the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (September 2014) and FDIC Circular 4010.3, *Enterprise Risk Management Program*, (dated April 16, 2012) emphasize the importance of policies and procedures as critical components of an effective internal control system.[8] Policies and procedures help ensure repeatable, consistent, and disciplined processes and reduce operational risk associated with changes in staff.

NIST Guide SP 800-47 recommends that agencies create a step-by-step approach for establishing system interconnections and verifying that the interconnections operate efficiently and securely. NIST Guide SP 800-47 also recommends that agencies define roles and responsibilities for establishing and maintaining system interconnections.

The CIO Organization issued policies, procedures, and templates for establishing system interconnections including:

- *Policy 12-005 on Data Network Security*, dated March 2012;
- *Rational Unified Process (RUP) Security Procedures*, dated May 2009;
- *System Development Life Cycle (SDLC) Security Procedures*, dated March 2017;
- *Firewall Change Request Process*, dated March 10, 2014, and updated April 5, 2017.

The FDIC also developed MOA and ISA templates that require key information about the interconnection, such as the systems to be interconnected, the type of information to be exchanged, and the requirements and procedures for reporting security incidents.

Based on our review of these existing policies and procedures, we found that the FDIC did not:

[7] FIPS Publication 200 defines minimum security requirements for Federal information and information systems.
[8] This circular was superseded in October 2018 and renamed FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program*.

- Define the types of technologies and configurations that could constitute a system interconnection and, therefore, require an MOA and ISA (or equivalent document);

- Define roles and responsibilities for all stakeholders involved in:

  - *Planning system interconnections*. Policies and procedures did not designate individual(s) within a Division or Office responsible for justifying the need for interconnections; establishing technical and security requirements; or creating agreements with the external organization to govern the management, operation, and use of the interconnection.

  - *Establishing system interconnections*. Policies and procedures did not designate individual(s) responsible for approving system interconnections and implementing and configuring security controls. Policies and procedures also did not define the role of the Legal Division in reviewing MOAs and ISAs for legal sufficiency.

  - *Maintaining system interconnections*. Policies and procedures did not designate individual(s) responsible for monitoring and testing interconnections to ensure they continue to operate properly and securely. They also did not address requirements for regularly communicating with outside organizations to ensure technologies and contacts in the agreements are up to date in case of a breach or technical connection issues and errors.

  - *Terminating system interconnections*. Policies and procedures did not designate individual(s) responsible for terminating interconnections when no longer required, or in response to an emergency, such as a system breach.

- Define documentation requirements for key activities, such as how the FDIC should notify outside organizations of its intent to terminate an interconnection. Policies and procedures also did not address who has responsibility for maintaining such documentation and for how long.

CIO Organization staff acknowledged that they had not established policies and procedures to address the activities described above because the number of system interconnections maintained by the FDIC has decreased in recent years. Nevertheless, the FDIC maintained 11 system interconnections that supported the transfer of significant amounts of sensitive information. Without adequate policies and procedures, the FDIC cannot be sure that these system interconnections are

effectively managed and secured, and that the terms of MOAs and ISAs will be implemented.

Absent complete policies and procedures, the FDIC cannot be sure that its employees and contractor personnel will understand their respective roles and responsibilities. In addition, the FDIC cannot properly manage, secure, maintain, and terminate system interconnections in a consistent manner; and retain proper documentation. Policies and procedures help to ensure the implementation of management's expectations and reduce operational risk associated with workforce staffing changes. For example, without current policies and procedures, the CIO Organization relies on the knowledge and experience of individual Federal staff and contractors for critical technical roles such as firewall administration. Should these individuals leave the FDIC, it may be difficult to obtain information about a system interconnection, such as when and why the FDIC implemented it and who approved it.

In addition, we identified instances in which the FDIC's lack of policies and procedures could have contributed to deficiencies, such as agreements expiring and system interconnections not being terminated in a timely manner. Without policies and procedures, staff may not routinely update agreements to ensure they remain current (e.g., include current references to the counterparties' contact information.) Further, staff may not understand management's expectations or their roles and responsibilities for terminating an agreement, notifying the outside organization, and ensuring that the system interconnection is removed from FDIC's firewall. For example, as described later, the FDIC had not established an agreement for one system interconnection, and thus could not provide any information about its business need or use. Developing and updating existing policies and procedures can also help the FDIC ensure that it establishes agreements for all system interconnections.

Recommendation

We recommend that the CIO:

1. Revise and update existing policies and procedures to address the Planning, Establishment, Maintenance, and Termination of system interconnections, including roles and responsibilities and documentation requirements.

Agreements for Certain Interconnections Not Established

NIST Guide SP 800-47 recommends that agencies establish MOAs and ISAs or an equivalent document to govern their system interconnections.[9] NIST Guide SP 800-47 states that organizations may choose to incorporate this information into a formal contract, especially if the organization is establishing the interconnection with a commercial organization. MOAs and ISAs are vital for protecting the confidentiality, integrity, and availability of interconnected systems and the data they process. These agreements define the responsibilities of each participating organization in interconnecting, operating, and securing the IT systems and include technical, security, and administrative requirements.

In May 2009, the CIO Organization issued the RUP Security Procedures, which required an MOA and ISA whenever the FDIC (1) transfers data outside the agency or (2) sends and receives data. However, the RUP Security Procedures did not require an MOA and ISA when the FDIC merely logged into an IT service (e.g., Website) to import data to the FDIC's systems and did not upload any data. In March 2017, the CIO Organization revised the RUP Security Procedures and renamed them the SDLC Security Procedures. The SDLC Security Procedures still required an MOA and ISA when the FDIC transferred data outside of the agency. However, the SDLC Security Procedures clarified that an MOA and ISA is required when the FDIC imports data through a constant network connection with an outside organization system (e.g., VPN), regardless of whether the FDIC also sends data to the outside organization.

Based on our work, we determined that the FDIC did not have ISAs for 18 percent of its system interconnections (2 of 11 interconnections), as required by the RUP Security Procedures in effect when the FDIC established those connections. Similarly, the FDIC did not have MOAs for 27 percent of its system interconnections (3 of 11 interconnections), as prescribed by the RUP Security Procedures in effect when the FDIC established those connections.

In addition, the CIO Organization could not provide any information about one system interconnection, including the date when the FDIC established the connection, the type of data that was exchanged, the security controls employed, or who approved the connection. Therefore, we could not determine whether the CIO Organization had complied with its procedures for establishing an MOA and ISA for the connection.

[9] OMB A-130, Appendix III, also requires Federal agencies to establish MOAs and ISAs whenever they interconnect their systems with outside organizations.

Table 2: System Interconnections With/Without MOAs and ISAs

Outside Organization	MOA Executed?	ISA Executed?	Date the MOA, ISA, or Contract was Signed
Organization 1	Yes	Yes	7/12/2016
Organization 2	No	Yes	3/24/2014
Organization 3	Yes	Yes	8/13/2009
Organization 4	Yes	Yes	10/21/2015 (MOA) 10/22/2015 (ISA)
Organization 5	Yes	Yes	11/14/2017(MOA) 11/1/2017 (ISA)
Organization 6	Yes	Yes	8/18/2014
Organization 7	Yes	Yes	9/21/2009
Organization 8	The FDIC could not provide information	The FDIC could not provide information	The FDIC could not provide information
Organization 9	No	No	The FDIC could not provide information
Organization 10	No	No	4/16/2009
Organization 11	Yes	Yes	6/5/2017

Source: OIG analysis of FDIC network firewall rules as of September 7, 2017 and the MOAs and ISAs.

We brought the exceptions for Organization 2, 9, and 10 in Table 2 to the attention of the CIO Organization during the audit. The CIO Organization expressed the view that the FDIC's system interconnections with Organizations 2 and 10 did not require an MOA or ISA because the FDIC had contracts with the associated vendors. The CIO Organization further asserted that these contracts contained standard contract clauses to protect the off-site storage of data, changes to the connections, and security incident reporting and, therefore, are equivalent to an MOA and ISA.

However, we reviewed the FDIC's contracts with Organizations 2 and 10 and noted that they both contained clauses stating "the contractor shall execute an Interconnection Security Agreement/Memorandum of Understanding with FDIC prior to establishing any data connection between the FDIC network and Contractor facility."[10] We also found that the contracts did not address the following elements of the FDIC's MOA and ISA templates:

- Details regarding the security controls required to be maintained by the parties to protect the connection and data;

- A system diagram or topological drawing[11] providing a visual depiction of the system interconnection, and;

[10] Section 7.4.2-03, Data Connection, July 2008 of the respective contracts.

[11] The FDIC ISA template uses the term system diagram instead of topological drawing; both terms depict the same information recommended by NIST Guide SP 800-47. According to NIST Guide SP 800-47, a topological drawing illustrates the connection between the interconnected systems as well as all communications paths, circuits, and other components. The drawing should also depict the location of all components.

- The approvals of the CIO and CISO accepting the risk and responsibility associated with the interconnections.[12]

When utilizing a contract to govern a system interconnection, the FDIC should ensure that contracts incorporate and address key elements of the MOA and ISA templates. The CIO Organization and the Division of Administration (DOA) share a responsibility for completing and executing contracts.

With regard to the FDIC's system interconnection with Organization 9, the CIO Organization asserted that the FDIC merely used the interconnection to download purchase card data to FDIC's New Financial Environment system. Therefore, because the connection did not involve uploading data to Organization 9, the former RUP Security Procedures did not require an MOA and ISA. In April 2018, the FDIC terminated the connection with Organization 9 after we brought it to the CIO Organization's attention during this audit, because it was determined the connection no longer served a business need.[13] Therefore, we did not conduct further work in this area.

Impact of Interconnections Without Agreements

Without an MOA or ISA (or equivalent document), the FDIC lacks an agreement for the management, operation, and use of the interconnection and accountability for the security controls required to protect the IT systems and data. This reduces the attention given by the organizations to required security controls. As a result, the interconnected IT systems and data may not be adequately protected and security risks may exist without the FDIC's knowledge. In addition, without an MOA and ISA (or equivalent document), organizations may not properly address the handling or reporting of security incidents involving system interconnections.

Further, without an MOA and ISA (or equivalent document), procedures do not exist for organizations to communicate changes to their IT environments. Such changes can include new security controls as well as changes to individuals' access rights to data, the electronic location of data, and key personnel contact information. If an organization makes changes without notifying the other organization, the system interconnection may not operate as intended, thereby affecting business needs and operations.

[12] NIST Guide SP 800-47 recommends that senior officials from each participating organization approve the system interconnection.
[13] Organization 9 serviced the FDIC's processing of purchase card transactions until the FDIC changed its service provider and established a new interconnection with Organization 5 in May 2008. The FDIC established an MOA and ISA with Organization 5, and updated that MOA and ISA in September 2017. Therefore, the connection with Organization 9 was no longer needed.

Recommendations

We recommend that the CIO:

2. Execute MOAs and ISAs with Organization 2 and Organization 10 in accordance with the relevant contracts.

3. Revise the standard contract language used for future contracts involving system interconnections, in coordination with DOA, to align with NIST guidance.

Expired FDIC Agreements Governing Interconnections

The RUP Security Procedures and SDLC Security Procedures require Division and Office ISMs to review MOAs and ISAs annually to ensure they remain current. In addition, the MOA and ISA templates state that these agreements should be updated and reauthorized prior to their expiration. The FDIC's MOAs have a 1 year base performance period, and renew for up to two additional 1 year renewal terms, unless either party terminates the agreement. Similarly, the FDIC's ISAs have a base period of performance of either 1 or 3 years, and automatically renew for up to 2 years. At the end of the base period and automatic renewal periods, the MOAs and ISAs expire. We found that:

- Four of the FDIC's eight ISAs (50 percent) had expired even though the underlying interconnection remained active;

- Three of the FDIC's seven MOAs (43 percent) had expired even though the underlying interconnection remained active;

- The MOAs and ISAs for two of the four interconnections expired in 2012, more than 4 years prior to our review; and

Table 3 summarizes the status of MOAs and ISAs that had expired at the time of our fieldwork.

Table 3: System Interconnections with Expired MOAs and/or ISAs

Outside Organization	Date MOA Established	Date ISA Established	Date Agreements Expired
Organization 2	×	3/24/2014	3/24/2017
Organization 3	8/13/2009	8/13/2009	8/13/2012
Organization 6	8/18/2014	8/18/2014	8/18/2017
Organization 7	9/21/2009	9/21/2009	9/21/2012

Source: OIG analysis of MOAs and ISAs as of January 31, 2018.

× The FDIC used a contract instead of an MOA.

We brought the exceptions in Table 3 to the attention of CIO Organization staff during the audit. On March 28, 2018, CIO Organization staff informed us that the FDIC was working to replace the expired ISA with Organization 2; establish a new MOA and ISA with a new organization, which acquired Organization 3 in March 2012; and replace its expired MOA and ISA with Organization 6. In addition, the interconnection with Organization 7 was no longer being used.

As previously discussed, when an MOA or ISA expire, the FDIC no longer has an agreement with the outside organization regarding the management, operation, and use of the system interconnection. Consequently, there is reduced accountability for the security controls required to protect the interconnection. Expired MOAs and ISAs increase the risk that current information would not be available to counterparties in the event of a breach or technical connection issue.

Outdated Information

NIST Guide SP 800-47 states that it is critical for both organizations involved in a system interconnection to maintain clear lines of communication and to ensure regular communication throughout the life-cycle of the interconnection. To facilitate this communication, NIST Guide SP 800-47 states that participating organizations should designate and provide contact information (e.g., telephone or e-mail) for the technical leads of their respective systems. Exchanging such contact information allows each organization to notify the other party in a timely manner of specific events, such as security incidents, disasters and other contingencies that disrupt the normal operation of the systems, and material changes to the systems' configurations. In addition, the FDIC's MOA and ISA templates state that frequent formal communications are essential to ensure the successful management of the interconnection. For example, technical changes to the interconnection and changes in contact information or long term absences of key points of contact should be communicated in writing.

Many of the MOAs and ISAs we reviewed did not contain current contact information. For example, seven ISAs and five MOAs we reviewed contained the names of key senior FDIC officials who provided authorization for the interconnection to operate but who no longer worked for the FDIC, or no longer held the position of CIO or CISO. The CIO Organization advised that contact information in MOAs and ISAs often becomes outdated because the outside organizations do not inform the FDIC of changes in staff. The Director, Division of Information Technology (DIT), stated that more frequent contact with the outside organizations could benefit the FDIC.

Outdated contact information can impede the FDIC's efforts to notify outside organizations in a timely manner of events covered in the MOA and ISA, including security incidents. In turn, this could delay the outside organization's efforts to

determine whether its system has been compromised and to take appropriate security precautions, exposing the FDIC to potential liability and reputational harm.

We identified two factors that contributed to the expired MOAs and ISAs and outdated contact information. First, we noted that Division and Office ISMs did not review MOAs and ISAs annually to ensure the information they contain remained current. Second, the CIO Organization did not periodically contact the outside organizations to determine whether changes had occurred that would require updates to the MOAs and ISAs.

Recommendations

We recommend that the CIO:

4. Ensure that Division and Office ISMs review MOAs and ISAs annually to ensure they remain current.

5. Implement procedures to regularly review, update, and reauthorize MOAs and ISAs, including contacting outside organizations when appropriate.

FDIC Interconnections Remained Enabled When No Longer Justified

NIST Guide SP 800-47 recommends that organizations terminate their system interconnections in a planned manner in order to avoid disrupting the other organization's system. This includes notifying the other organization of the intent to terminate the interconnection.

The CIO Organization did not terminate 27 percent of its system interconnections (3 of 11 interconnections) in a timely manner. In response to our inquiries during this audit, CIO Organization staff determined that there was not a business need for the interconnections with Organizations 7, 8, and 9. As a result, the CIO Organization terminated these interconnections in March and April 2018. We noted that the FDIC stopped using its interconnection with Organizations 7 and 9 in 2017 and 2008, respectively. As explained earlier in this report, CIO Organization staff could not provide us with information about the interconnection with Organization 8, including when the FDIC stopped using the connection.

A firewall administrator in the CIO Organization informed us that a quarterly review of the network firewall rules is conducted and rules that are no longer needed are removed. However, this review was not effective. Had the review process worked as intended and identified rules no longer needed, the FDIC should have removed the aforementioned interconnections. We are currently reviewing this process as part of a broader audit of *Controls for Preventing and Detecting Cyber Threats* and will separately report the audit results.

Not terminating system interconnections in a timely manner exposes the FDIC to increased security risks. For example, a malicious insider could use an unmonitored interconnection to access sensitive FDIC data, or as a conduit to compromise the other organization's system.

FDIC Lacked a Formal Notification Process for Terminations

In addition, the FDIC did not have a formal process to notify outside organizations of the intent to terminate a system interconnection and did not provide written notices of termination. However, NIST Guide SP 800-47 recommends that when either organization in a system interconnection wishes to terminate the connection, they should provide advance written notice to the other party and receive an acknowledgment in return. Such notification includes the reason for the termination, a proposed timeline for the disconnection, and the identification of staff who will conduct the disconnection.

We found that the FDIC terminated the three system interconnections noted above in March and April 2018 without notifying the outside organizations. The CIO Organization expressed the view that notification to the counterparties was unnecessary for these system interconnections because the FDIC's MOAs and ISAs with the organizations stated that "this agreement shall automatically terminate at such time as the purpose for which the interconnection was created ceases to exist and the connection is terminated." Notably, the FDIC only had an MOA and ISA in place for one of the three terminated system interconnections (Organization 7) that contained similar language. The other two system interconnections (Organization 8 and Organization 9) did not have an MOA, ISA, or equivalent agreement in place that contained such language when the CIO Organization terminated the connections.

In addition, the CIO Organization did not terminate the system interconnection with Organization 7 until March 2018, after the OIG brought it to their attention. Therefore, although the purpose for which the system interconnection was established ceased to exist, the FDIC had not timely terminated the connection. In addition, the MOA and ISA automatically terminated, however, the connection remained active.

If the FDIC does not provide written notification to a counterparty of its intent to terminate a system interconnection, the counterparty may not be aware there is no longer a business need for the interconnection and may not terminate the interconnection on their end. System owners and technical staff then cannot undertake appropriate preparations, such as notifying affected users, determining how shared data will be disposed of, and updating documents (e.g., system security plans) to reflect the changed IT environment.

Recommendation

We recommend that the CIO:

6. Develop and implement procedures for providing written notification to technical staff within the FDIC and at outside organizations when a system interconnection is no longer needed.

Secure File Transfers and Secure Sockets Layer VPNs

During the course of our work, we learned that although outside the scope of our audit, the FDIC utilizes certain types of technologies to exchange data with outside organizations that are not specifically addressed in NIST Guide SP 800-47 and that the CIO Organization does not consider to be system interconnections. These technologies include secure file transfer (SFT) and secure sockets layer VPNs (SSL VPN). We also noted that the FDIC had not fully developed policies and procedures addressing secure data transport utilizing technologies that are not system interconnections. Such policies and procedures are important to ensure that FDIC personnel understand the proper usage of technologies available to facilitate data exchange and implement adequate safeguards to protect sensitive FDIC data being shared.

Secure File Transfer

Based on interviews with CIO Organization staff and review of CIO Organization guidance, we learned that in recent years, the FDIC has increased its use of SFTs. The FDIC often utilizes file management software products to facilitate SFTs of large data files with outside organizations. For example, in January 2018, the FDIC changed its transmission method for exchanging credit card transaction information with Organization 5 from a system interconnection utilizing a VPN to a SFT.

In 2016, the CIO Organization established the *Secure File Transfer with External Stakeholders - Interim Guidance* (File Transfer Interim Guidance) to "better educate users on the use of these technologies and to stop the outflow of sensitive information to unknown end-points." The File Transfer Interim Guidance acknowledged that the CIO Organization had received an increasing number of requests to exchange files that contain sensitive data. The Guidance states that using SFT poses risk both to the data and the organization. For example, the Guidance states that data is only protected while in transit, and not after it is received by an outside organization. In addition, the Guidance states that if the outside organization does not bring the data into its internal network, but stores the data on the SFT site instead, the only barrier between an attacker and the data is a User ID and password to access the SFT site. Therefore, an attacker could gain access to the FDIC's data within an SFT site using a compromised User ID and password

because an SFT only protects data while it is in transit. The File Transfer Interim Guidance adds that if the data is removed from the SFT site and brought under the protection of the organization's internal network, theoretically, it is more secure.

Secure Sockets Layer VPNs

The FDIC has also used SSL VPNs to transfer and receive data with outside organizations. NIST Guide SP 800-47 does not explicitly address SSL VPNs. However, these connections may be considered a system interconnection if the connection is configured in a manner where two or more IT systems are directly connected.

NIST issued *Guide to SSL VPNs* (SP 800-113) in July 2008, which cites risks for SSL VPNs that are similar to those associated with system interconnections. Such risks include encryption weaknesses that could allow an attacker to intercept and decrypt the data while in transit, as well as an attacker posing as a legitimate user. During the course of our audit, we identified the following SSL VPN connections that the FDIC had established:

- Organization A: The FDIC established a connection with a vendor to provide phone communications maintenance support related to the move of the FDIC's Kansas City Regional Office.

- Organization B: The FDIC established a connection with a vendor to assist in monitoring network traffic (i.e., electronic communications) for potential network attacks.

- Organization C: The FDIC could not provide an explanation regarding why or when it initially established its connection with Organization C.

At the close of the audit, the FDIC had terminated the three SSL VPNs we brought to their attention. Nevertheless, the FDIC should assess any current or future SSL VPNs to identify any that are configured or operate in a manner that constitutes a system interconnection. If the FDIC identifies SSL VPNs that are system interconnections, it should put in place appropriate controls to govern the interconnections consistent with its other system interconnections. NIST Guide SP 800-47 emphasizes that it is important for agencies to protect their data regardless of how it is transferred.

Recommendation

We recommend that the CIO:

7. Develop and implement policies and procedures to govern the secure transfer of data outside of the FDIC using technologies that are not considered system interconnections.

FDIC COMMENTS AND OIG EVALUATION

The CIO Organization provided a written response, dated November 19, 2018, to a draft of this report. The response is presented in its entirety in Appendix 4. The CIO Organization concurred with six of the report's seven recommendations and partially concurred with the remaining recommendation. The CIO Organization described alternative corrective actions that it plans to take to address the remaining recommendation. The CIO Organization expects to complete corrective actions to address all seven recommendations by September 30, 2019. The recommendations will remain open until the OIG confirms that corrective actions have been completed and are responsive. Appendix 5 contains a summary of FDIC's corrective actions.

Objective

The objective of the audit was to assess the FDIC's controls for managing system interconnections with outside organizations. The audit focused on the FDIC's controls for planning, establishing, maintaining, and terminating system interconnections.

We conducted this performance audit from November 2017 through March 2018 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 March 19, 2018.

Scope and Methodology

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

- OMB Circular A-130, *Managing Information as a Strategic Resource,* issued July 2016;
- NIST Guide SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, issued August 2002;
- NIST Guide SP 800-122, *Guide for Protecting the Confidentiality of Personally Identifiable Information (PII),* issued April 2010;
- NIST Guide SP 800-37, *A Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, issued June 2014;
- NIST Guide SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, issued April 2013; and
- NIST Guide SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans,* issued December 2014.

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

- *Policy 12-005 on Data Network Security*, dated March 2012;
- *Firewall Change Request Process*, dated April 2017;
- MOA and ISA Templates, dated December 2017 and July 2014 respectively;
- Circular 4010.3, *Enterprise Risk Management Program*, dated April 2012;
- *Rational Unified Process Security Procedure*, dated May 2009; and
- *System Development Life Cycle Security Procedures*, dated March 2017.

Further, we interviewed FDIC officials to determine roles, responsibilities, and perspectives related to system interconnections. Such officials included the:

- CIO,
- Director, DIT,
- Firewall administrators,
- ISMs and
- Various FDIC Division staff as necessary.

Further, we reviewed the FDIC's records and activities related to planning, establishing, maintaining, and terminating system interconnections including reviewing documentation such as MOAs, ISAs, and contractual agreements. We also engaged the professional services firm of Cotton & Company LLP to assist the OIG in identifying FDIC's system interconnections with outside organizations. Cotton & Company LLP identified dedicated or leased lines, VPNs, and Connect: Direct connections.

Our audit work did not include assessing: (1) the accuracy and sufficiency of information in MOAs, ISAs, and contractual agreements (e.g., whether the implementation and use of the system interconnection was in accordance with the

agreements with respective to security, type of data being exchanged, individuals authorized to access data, and permitted uses of the data); (2) whether the FDIC implemented system interconnections as approved by senior management (e.g., provided FDIC users and outside organizations secure encrypted connections to specific data and systems to meet business needs); (3) the FDIC's processes for reviewing firewall rules to determine whether the business need for system interconnections still exists, (4) FDIC's procedures for monitoring network activity, including unusual activity associated with system interconnections, and (5) whether the FDIC maintained audit logs that recorded network activity and captured key data for its system interconnections as required by its ISAs with outside organizations. Our audit work also did not include contacting outside organizations involved in system interconnections.

We did not rely upon computer-processed information in the scope of our audit. Regarding compliance with laws and regulations, we analyzed FDIC's compliance with relevant provisions of OMB circulars and memorandums pertaining to system interconnections. In addition, we assessed the risk of fraud and abuse related to our objective in the course of evaluating audit evidence.

We performed our work at the FDIC's Headquarters offices in Washington, D.C., and at Virginia Square in Arlington, Virginia.

Appendix 2 Glossary

Term	Definition
Authentication	The process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. [NIST Guide SP 800-47]
Authorization to Operate	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations. [NIST Guide SP 800-47]
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. [FDIC OIG Report No. AUD-17-006]
Dedicated Line	A leased or privately owned transmission line that provides a constant transmission path from point A to point B. [NIST Guide SP 800-47]
Encryption	The translation of data into a form that is unintelligible without a deciphering mechanism. [NIST Guide SP 800-47]
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. [NIST Guide SP 800-47]
Information Resources	Information and related resources, such as personnel, equipment, funds, and IT. [44.U.S.C.§ 3502]
Information Security Manager	An individual assigned to ensure entire divisional compliance with FDIC security policies, implement business-specific security practices, and serve as primary liaison between the CIO Organization and the ISM's Division/Office. [FDIC Circular 1360.12, *Reporting Information Security Incidents*]
Internal Control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. [GAO's *Standards for Internal Control in the Federal Government]*
National Institute of Standards and Technology	Founded in 1901, NIST is a non-regulatory Federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement, science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST issues publications on IT usage and best practices, including cloud computing. NIST is responsible for developing information security standards and guidelines. [NIST.gov]
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identify either alone or when combined with other information that is linked or linkable to a specific individual. [OMB Circular A-130]
Rational Unified Process	A commercial-off-the-shelf process framework that is expected to be tailored to meet the specific needs of projects based on size, scope, risk, and complexity. [FDIC CIO Organization IT Governance Frameworks and Methodologies]
Secure File Transfer	A secure service that supports file transfer between computers. [NIST Guide SP 800-47 and NIST Guide SP 800-82 Revision 2]
Secure Sockets Layer VPN	A virtual network that provides secure remote access to an organization's resources. SSL VPNs consist of one or more VPN devices to which users connect using their Web browsers. [NIST Guide SP 800-113]
Security Controls	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [OMB Circular A-130]

Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [NIST Guide SP 800-53, Revision 4]
Systems Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal. [NIST Guide SP 800-137]

Appendix 3 Acronyms and Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
DOA	Division of Administration
DIT	Division of Information Technology
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
IPsec	Internet Protocol Security
ISA	Interconnection Security Agreement
ISM	Information Security Manager
IT	Information Technology
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RUP	Rational Unified Process
SDLC	Systems Development Life Cycle
SFT	Secure File Transfer
SP	Special Publication
SSL	Secure Sockets Layer
VPN	Virtual Private Network

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500 Office of the Chief Information Officer

DATE: November 19, 2018

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

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

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

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

SUBJECT: Management Response to the Draft Audit Report Entitled *Controls Over System Interconnections with Outside Organizations* (Assignment No. 2017-026)

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the Federal Deposit Insurance Cooperation's (FDIC) Controls over System Interconnections with Outside Organizations issued November 5, 2018. We value the independent insights and opinions of the audit team and the perspective they provided to the Chief Information Officer Organization (CIOO).

We appreciate the OIG's evaluation, and we expect that the actions taken in response to this draft report will further enhance the FDIC's management of system interconnections with outside organizations. The Corporation has taken action to renew expired Memorandum of Agreements (MOA) and Interconnection Security Agreements (ISA). In addition, FDIC completed efforts to terminate connections with outside organizations that no longer serve a business need. During the course of the audit, CIOO established a working group to streamline the revision of existing system interconnection policies and procedures to ensure FDIC properly manages, secures, maintains, and terminates system interconnections in a consistent manner.

In its report, the OIG audit team made seven (7) recommendations to the CIOO. We have carefully considered and concur with six (6) recommendations, and partially concur with one (1) recommendation where we include alternative action(s) to address the audit recommendation. This response outlines the CIOO's completed or planned corrective actions and the expected completion dates.

We look forward to productive discussions with the OIG in the coming months regarding the FDIC's efforts to address the areas identified in the report.

MANAGEMENT RESPONSE

Recommendation 1

We recommend that the CIO:

1. Revise and update existing policies and procedures to address the Planning, Establishment, Maintenance, and Termination of system interconnections, including roles and responsibilities and documentation requirements.

   Management Decision: Concur

   Corrective Action:

   At the time of this audit's field work, OCISO established a working group to document the interconnection security agreement process and lifecycle management of these agreements. Based on this process improvement effort, OCISO will revise and update existing policies and procedures to address the planning, establishment, maintenance, and termination of system interconnections, including roles and responsibilities and documentation requirements.

   Estimated Completion Date: April 30, 2019

Recommendation 2

We recommend that the CIO:

2. Execute MOAs and ISAs with Organization 2 and Organization 10 in accordance with the relevant contracts.

   Management Decision: Partially Concur

   Corrective Action:

   FDIC executed a MOA and ISA with Organization 2 on May 10, 2018.

   Organization 10 was originally established as an IPSec VPN to secure web communication to the offsite-hosted system and to ensure that connections could only be established from the FDIC's network. When the contract came up for renewal, the need for a VPN was re-assessed and it was determined that the secure FDIC network-only originating communication requirements could be achieved via TLS and IP-whitelisting solution. This connection is managed/controlled by the FDIC and Organization 10 does not have responsibilities for its use, operation, or maintenance that would require their signatures on an MOA and ISA. The current contract language with Organization 10 incorrectly includes the requirement to execute an

ISA/MOA with FDIC therefore we partially concur and have established an alternate course of action. FDIC will work with DOA to review and revise existing standard contract language to remove this requirement.

Estimated Completion Date: September 30, 2019

Recommendations 3

We recommend that the CIO:

3. Revise the standard contract language used for future contracts involving system interconnections, in coordination with DOA, to align with NIST guidance.

Management Decision: Concur

Corrective Action:

OCISO will revise and update existing policies to ensure relevant contracts incorporate and address key elements of the MOA and ISA templates to align with NIST guidance. OCISO will provide DOA with standard contract clause language to be implemented in the standard contract language used for future contracts involving system interconnections once the revised policy has been finalized.

Estimated Completion Date: September 30, 2019

Recommendation 4

We recommend that the CIO:

4. Ensure that Division and Office ISMs review MOAs and ISAs annually to ensure they remain current.

Management Decision: Concur

Corrective Action:

CIOO will develop a Standard Operating Procedure that requires FDIC ISMs review MOAs and ISAs annually to ensure they remain current.

Estimated Completion Date: May 31, 2019

3

Recommendation 5

We recommend that the CIO:

5. Implement procedures to regularly review, update, and reauthorize MOAs and ISAs, including contacting outside organizations when appropriate.

Management Decision: Concur

Corrective Action:

OCISO will revise existing procedures and implement the modified procedures to regularly review, update, and reauthorize MOAs and ISAs, including contacting outside organizations when appropriate.

Estimated Completion Date: April 30, 2019

Recommendation 6

We recommend that the CIO:

6. Develop and implement procedures for providing written notification to technical staff within the FDIC and to outside organizations when a system interconnection is no longer needed.

Management Decision: Concur

Corrective Action:

OCISO will revise existing procedures and the implement modified procedures to include requirements for providing written notification to technical staff within the FDIC and to outside organizations when a system interconnection is no longer needed.

Estimated Completion Date: April 30, 2019

Recommendation 7

We recommend that the CIO:

7. Develop and implement policies and procedures to govern the secure transfer of data outside of the FDIC using technologies that are not considered system interconnections.

4

Management Decision: Concur

Corrective Action:

OCISO rescinded the interim guidance titled "Secure File Transfer with External Stakeholders" which was outdated and did not reflect FDIC's secure file transfer usage requirements on November 16, 2018. OCISO will revise existing procedures to include requirements for governing the secure transfer of data outside of the FDIC using technologies that are not considered system interconnections.

Estimated Completion Date: September 30, 2019

If you have any questions regarding this response, please contact Kim Farrell, Acting Chief, Audit and Internal Control Section, DIT at 703-516-5101.

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Controls
Greg Kempic, DOF, Risk Management and Internal Controls
Mittal Desai, Deputy Chief Information Security Officer
Farhan H. Khan, Acting Deputy Director, DIT, Business Administration Branch

5

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The OCISO will revise and update existing system interconnection policies and procedures to address all four phases of the NIST life-cycle framework, including roles and responsibilities and documentation requirements.	April 30, 2019	No	Yes	Open
2	The FDIC executed an MOA and ISA with Organization 2 on May 10, 2018. In addition, the CIO Organization determined that it no longer needed a system interconnection to support the exchange of data with Organization 10 and replaced the interconnection with a different IT solution. The CIO Organization will work with DOA to revise the existing contract language to remove the requirement for an MOA and ISA.	September 30, 2019	No	Yes	Open
3	The OCISO will revise existing policies to ensure relevant contracts address key elements of the MOA and ISA templates consistent with NIST guidance. In addition, the OCISO will provide DOA standard contract language for inclusion in future contracts involving system interconnections.	September 30, 2019	No	Yes	Open
4	The CIO Organization will develop a Standard Operating Procedure that requires ISMs to review MOAs and ISAs annually to ensure they remain current.	May 31, 2019	No	Yes	Open
5	The OCISO will revise and implement procedures to regularly review, update, and reauthorize MOAs and ISAs, including contacting outside organizations when appropriate.	April 30, 2019	No	Yes	Open
6	The OCISO will revise and implement procedures to provide written notification to technical staff within the FDIC and to outside organizations when a system interconnection is no longer needed.	April 30, 2019	No	Yes	Open

7	The OCISO rescinded the interim guidance, entitled *Secure File Transfer with External Stakeholders*. The OCISO will revise existing procedures to include requirements for governing the secure transfer of data outside of the FDIC using technologies that are not considered system interconnections.	September 30, 2019	No	Yes	Open

[a] Recommendations are resolved when —

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

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

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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