Office of Inspector General

Preventing and Detecting Cyber Threats

May 2019 AUD-19-005

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

REDACTED VERSION

PUBLICLY AVAILABLE

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

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

NOTICE

On June 7, 2019, the Office of Inspector General made minor changes on page 2 of the report to clarify the timing and targets of an Advanced Persistent Threat that affected the FDIC. This clarification did not affect the report's findings, conclusions, or recommendations.

Executive Summary

Preventing and Detecting Cyber Threats

According to the Department of Homeland Security, cyber threats remain one of the most significant strategic risks facing the United States. Every day, Federal agencies defend their information systems and data against cyber attacks by malicious actors. According to the Office of Management and Budget, Federal agencies experienced 35,277 cybersecurity incidents during Fiscal Year 2017. This number represented a 14-percent increase over the 30,899 incidents that Federal agencies experienced in Fiscal Year 2016. In addition to addressing a growing number of cyber threats, Federal agencies must address increasingly sophisticated threats.

Following a series of data breaches at the FDIC in late 2015 and 2016, the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs raised concerns about the FDIC's information technology (IT) systems, and we initiated this audit. The audit focused on two security controls intended to prevent and detect cyber threats on the FDIC's network: (i) Firewalls; and (ii) the Security Information and Event Management (SIEM) tool. The FDIC's firewalls and SIEM tool operate in concert with other network security controls as part of a defense-in-depth cybersecurity strategy.

The FDIC has deployed firewalls at the perimeter and interior of its network to control the flow of information into, within, and out of the network. These network firewalls use rules that enforce what traffic is permitted. Firewalls are only as effective as the rules that organizations define for them.

The FDIC has implemented a SIEM tool that operates within the network to analyze network activity and detect indications of potential cyber threats that may have bypassed the firewalls and other security controls. The FDIC's SIEM tool collects audit log data generated by network IT devices and ran [redacted] automated queries known as Use Cases to identify specific types of events or patterns of activity that may indicate a cyber attack is occurring. When a Use Case detects suspicious activity, the SIEM tool sends an alert to the FDIC's Computer Security Incident Response Team for further investigation.

The audit objective was to assess the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. We engaged the

professional services firm of Cotton and Company LLP to perform much of the audit planning and field work.

Results

We identified weaknesses that limited the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. With respect to firewalls, we identified weaknesses in the following areas:

- Many firewall rules lacked a documented justification, and the majority of firewall rules ([redacted]) were unnecessary. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need.

- Firewalls did not comply with the FDIC's minimally acceptable system configuration requirements. In addition, the FDIC did not update its minimum configuration requirements in a timely manner to address new security configuration recommendations approved by the National Institute of Standards and Technology.

- The FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls. In addition, [redacted]

- [redacted].

We notified the FDIC's Chief Information Officer (CIO) and then-Acting Chief Information Security Officer (CISO) of concerns regarding the administration of the network firewalls during the audit. The CIO and then-Acting CISO concurred with our concerns and stated that the CIO Organization was taking corrective actions.

With respect to the SIEM tool, we found that the FDIC properly set up the tool to collect audit log data from key network IT devices. In addition, the SIEM tool effectively formatted that data to allow for analysis of potential cyber threats. However, the FDIC did not have a written process to manage the ongoing identification, development, implementation, maintenance, and retirement of Use Cases for the SIEM tool. In addition, [redacted] Use Cases used by the SIEM tool were [redacted]

[redacted].

Recommendations

Our report contains 10 recommendations intended to strengthen the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. In a written response to the report, the CIO Organization concurred with all ten recommendations.

Following the issuance of the draft report, the CIO Organization provided us with corrective action documentation for 8 of the 10 recommendations. We determined that the documentation was responsive for four of the eight recommendations and closed them. We plan to review the corrective action documentation for the other four recommendations as part of our audit follow-up process. The CIO Organization plans to complete corrective actions for the report's remaining two recommendations by January 31, 2020.

Contents

Background **3**

Federal Statutes, Policies, and Guidelines 5
Network Firewalls 6
Security Information and Event Management Tool 8

Audit Results **11**

Firewall Rules Lacked Key Documentation 12
Numerous Firewall Rules Were Unnecessary 13
Firewalls Did Not Comply with Baseline Configurations 19
Baseline Configurations Were Outdated 20
Controls Over Access to Local Firewall Accounts Were Ineffective 21
Restrictions on Access to Network Firewalls Were Inadequate 24
Process for Managing SIEM Tool Use Cases Needed Improvement 25
Certain SIEM Tool Use Cases Did [redacted] 29

FDIC Comments and OIG Evaluation **30**

Appendices

1. Objective, Scope, Methodology 31
2. Glossary 35
3. Acronyms and Abbreviations 38
4. Prior Security Weaknesses and Recommendations Related to Firewall Rules 39
5. OIG Memorandum Regarding the Administration of Network Firewalls 41
6. Management's Response to OIG Memorandum Regarding the Administration of Network Firewalls 44
7. FDIC Comments 58
8. Summary of the FDIC's Corrective Actions 65

Figures

1. Network Firewall Architecture 8
2. Implementation of the FDIC's SIEM Tool 10
3. Use Case Management Process 27

May 28, 2019

Howard G. Whyte
Chief Information Officer and Chief Privacy Officer

Subject | ***Preventing and Detecting Cyber Threats***

According to the Department of Homeland Security (DHS), cyber threats[1] remain one of the most significant strategic risks facing the United States.[2] Cyber threats can come from both internal and external sources. Internal threats may include insider threats or fraudulent or malevolent acts by employees or contractors who work for the Federal Deposit Insurance Corporation (FDIC). External threats include a growing number of sophisticated cyber attacks that come from criminals, hackers, foreign nations, terrorists, and other adversaries. Cyber threats place our nation's security, economic prosperity, and public health and safety at risk.

Every day, Federal agencies defend their information systems and data against cyber attacks by malicious actors. Between 2006 and 2015, the number of cyber incidents reported to DHS that involved Federal information systems increased more than ten-fold.[3] Further, according to the Office of Management and Budget (OMB), Federal agencies experienced 35,277 cybersecurity incidents during Fiscal Year (FY) 2017.[4] This number represented a 14-percent increase over the 30,899 incidents that Federal agencies experienced in FY 2016.

In addition to addressing a growing number of cyber threats, Federal agencies must address increasingly sophisticated threats. A high-profile intrusion into the systems of the Office of Personnel Management (OPM) in 2015 illustrated the potential impact of a sophisticated cyber threat. According to the Government Accountability Office (GAO), this intrusion compromised the personnel records of over 4 million Federal employees, and ultimately affected nearly 22 million people.[5]

---

[1] The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-150, *Guide to Cyber Threat Information Sharing*, (Oct. 2016) defines the term cyber threat as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service." Certain terms that are underlined when first used in this report are defined in Appendix 2, *Glossary*.
[2] *Mitigating America's Cybersecurity Risk: Hearing Before S. Comm on Homeland Security & Gov. Affairs*, 115th Cong. (April 24, 2018), (statement of Jeanette Manfra, Assistant Secretary, National Protection and Programs Directorate, Office of Cybersecurity and Communications, DHS).
[3] DHS, *Cybersecurity Strategy* (May 15, 2018).
[4] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, FY 2017.
[5] GAO Report, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed* (GAO-17-614) (August 2017).

Since 1997, GAO has placed the security of Federal cyber assets on its High-Risk List.[6] Further, GAO has made more than 3,000 recommendations since 2010 aimed at addressing cybersecurity shortcomings at Federal agencies, and approximately 1,000 of these recommendations had not been implemented as of August 2018. GAO reported that "until these shortcomings are addressed, Federal agencies' information and systems will be increasingly susceptible to the multitude of cyber-related threats that exist."[7]

The FDIC relies heavily on information systems to carry out its mission of insuring deposits, supervising insured financial institutions, and resolving failed insured financial institutions. These systems contain sensitive information such as personally identifiable information (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. Absent effective controls for safeguarding its information systems and data, the FDIC is at increased risk of a cyber attack that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, sensitive information. Such an attack could threaten the FDIC's ability to accomplish its mission of ensuring the safety and soundness of institutions and maintaining stability in our Nation's financial system.

In 2010, the FDIC began to experience sophisticated, targeted attacks on its network known as an advanced persistent threat (APT), whereby an entity gained unauthorized access to the network, escalated its privileges, and developed an ongoing presence, thus compromising network data and component-level security. The attacker behind the APT penetrated more than 90 workstations or servers within the FDIC's network, including computers used by a former Chairman and other senior FDIC officials. The attacker also gained unauthorized access to sensitive FDIC data.

In December 2012, the FDIC engaged a consulting firm to investigate the APT and provide recommendations for better safeguarding the FDIC's information technology (IT) environment against future cyber attacks. In September 2013, the consulting firm issued a report, which recommended that the FDIC evaluate the feasibility of implementing a set of 23 recommendations that apply to most victims of targeted attacks. [redacted]

[6] Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that it considers high risk due to vulnerabilities to fraud, waste, abuse, and mismanagement, or a need for transformation. GAO places these agencies and program areas on its High-Risk List.
[7] GAO Report, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation* (GAO-18-622) (September 2018).

[redacted] According to the Chief Information Officer Organization (CIOO), as of December 1, 2017, the FDIC had taken action to address 21 of the 23 recommendations.[8] The CIOO determined that the remaining two recommendations were not feasible for the FDIC's business environment.[9]

Following a series of data breaches at the FDIC in late 2015 and 2016, the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs raised concerns about the FDIC's IT systems, and we initiated this audit. The audit focused on two security controls intended to prevent and detect cyber threats on the FDIC's network: (i) Firewalls; and (ii) the Security Information and Event Management (SIEM) tool. The FDIC's network firewalls serve as a first line of defense in preventing cyber threats by controlling the flow of information into and out of the network. The SIEM tool operates within the network to analyze network activity and detect indications of potential cyber threats that may have bypassed the firewalls and other security controls.

The audit objective was to assess the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. We engaged the professional services firm of Cotton and Company LLP to perform much of the audit field work. We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report provides additional details about our objective, scope, and methodology; Appendix 2 contains a glossary of terms; Appendix 3 contains a list of acronyms and abbreviations; Appendix 4 describes weaknesses related to firewall rules identified in prior FDIC security assessments; Appendix 5 contains a memorandum that the Office of Inspector General (OIG) issued to the FDIC's Chief Information Officer (CIO) during the audit regarding the administration of the network firewalls; Appendix 6 contains management's response to the OIG memorandum; and Appendices 7 and 8 contain the FDIC's comments and a summary of the FDIC's corrective actions, respectively.

BACKGROUND

From October 2014 through September 2017, the FDIC reported a total of 985 IT security incidents[10] to the former United States Computer Emergency Readiness

[8] We did not independently assess the adequacy of the FDIC's actions to address the recommendations.
[9] The information provided by the CIOO indicated that mitigating controls were in place for these two remaining recommendations.
[10] The FDIC's annual Federal Information Security Modernization Act (FISMA) submissions to OMB for FYs 2015 through 2017.

Team (US-CERT).[11] The FDIC classified 12 of these incidents as "major incidents," as defined in OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015.[12] Collectively, these major incidents involved the PII of more than 120,000 individuals, as well as business proprietary and sensitive data on financial institutions.

We issued two separate reports describing how the FDIC handled these breaches and other security incidents: *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (PII Audit Report)[13] and *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (Special Inquiry Report).[14] The PII Audit Report found that the FDIC did not have adequate controls for addressing breaches or notifying individuals affected by breaches in a timely manner. This report contained seven recommendations intended to promote more timely breach response activities and strengthen controls for evaluating the risk of harm to individuals potentially affected by a breach and notifying and providing services to those individuals, when appropriate. The FDIC implemented these recommendations.

The Special Inquiry Report found that the FDIC's reporting of major incidents to the Congress should have been more timely and precise. The report also revealed certain systemic weaknesses that hindered the FDIC's ability to handle multiple information security incidents and breaches efficiently and effectively. The Special Inquiry Report contained 13 recommendations to address the systemic issues associated with the FDIC's incident response and reporting and interactions with the Congress. As of March 2019, twelve recommendations had been implemented, and the remaining recommendation had not yet been implemented.

In July 2016, we also issued two audit reports that examined the FDIC's handling of security incidents: *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (Resolution Plan Report)[15] and *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (Major

[11] In 2017, US-CERT merged into the National Cybersecurity and Communications Integration Center (NCCIC). NCCIC is an organization within DHS. NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the Nation's critical IT and communications networks.
[12] OMB subsequently revised the definition of major incident in OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements* (Nov. 4, 2016). OMB currently defines major incident as "any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."
[13] OIG Report, *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (FDIC OIG AUD-17-006) (September 2017).
[14] OIG Report, *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (FDIC OIG 18-001) (April 2018).
[15] OIG Report, *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (FDIC OIG AUD-16-003) (July 2016).

Incident Report).[16] The Resolution Plan Report described a series of factors that contributed to a security incident involving a former FDIC employee who stole sensitive resolution plan information from the FDIC in 2015. Such factors included the lack of an insider threat program and weak security controls. The report contained six recommendations to safeguard sensitive resolution plans, which have been implemented by the FDIC.

The Major Incident Report found that the FDIC did not have adequate controls to properly identify, effectively address, or timely and accurately report major incidents. The Major Incident Report included five recommendations intended to strengthen the FDIC's ability to identify and report major information security incidents consistent with FISMA requirements and OMB policy. The FDIC implemented these recommendations.

The FDIC's 2018 Annual Report states that cybersecurity continues to be a top management priority at the FDIC. The Annual Report describes the FDIC's actions to strengthen and expand its cybersecurity program and practices in such areas as risk management, infrastructure resiliency, and IT governance.[17] Further, the FDIC's IT Strategic Plan includes a goal to improve information security and privacy protections against cyber threats and data breaches.[18] In support of this goal, the FDIC has undertaken a number of priority initiatives, such as implementing a Data Protection Program, testing required controls underlying the NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[19] and developing an enterprise security architecture.

Federal Statutes, Policies, and Guidelines

FISMA requires Federal agencies, including the FDIC, to develop, document, and implement an agency-wide information security program to protect their information and information systems. The statute directs NIST to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information systems. NIST establishes required security standards in Federal Information Processing Standard (FIPS) Publications. NIST supplements these standards with recommended guidelines in its SPs.[20]

---

[16] OIG Report, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (FDIC OIG AUD-16-004) (July 2016, Revised February 2017).
[17] FDIC, *2018 Annual Report* (February 2019).
[18] FDIC, *Information Technology Strategic Plan: 2017-2020.*
[19] NIST's *Framework for Improving Critical Infrastructure Cybersecurity* contains a set of industry standards and best practices to help organizations manage their cybersecurity risks. The President's Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, dated May 11, 2017, requires that Federal agencies use this Framework to manage their cybersecurity risks.
[20] It is the FDIC's position that NIST SPs contain statements of best practices or guidance and are not binding on the FDIC.

In September 2009, NIST issued SP 800-41, *Guidelines on Firewalls and Firewall Policy*, to assist Federal agencies in developing firewall policies and selecting, configuring, testing, deploying, and managing their firewalls.[21] In addition, NIST issued SPs 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations;* and 800-92, *Guide to Computer Security Log Management*; in April 2013, September 2011, and September 2006, respectively. Collectively, these NIST SPs provide agencies with guidelines regarding the use of SIEM tools.

OMB also issued government-wide information security-related policies and guidance that Federal agencies must follow. On July 28, 2016, OMB issued a revised Circular No. A-130, *Managing Information as a Strategic Resource*,[22] which defined responsibilities for protecting Federal information resources and managing PII.

Network Firewalls

According to NIST, firewalls are essential devices or programs that help organizations protect their networks and information systems from hostile attacks, break-ins, and malicious software.[23] Firewalls act as a safeguard by blocking network traffic that is not consistent with access requirements defined by the organization. Firewalls operate in concert with other network security controls, such as data loss prevention programs, as part of a defense-in-depth cybersecurity strategy.[24] According to NIST, a defense-in-depth strategy involves establishing multiple defensive barriers through integrated technology and operations in order to form a layered security architecture.

NIST recommends that agencies establish a firewall policy that is implemented through rules that enforce what traffic is permitted. According to NIST SP 800-41, firewalls should block all inbound and outbound traffic that is not expressly permitted by the firewall policy. This practice, known as “deny by default,” limits network traffic only to what is necessary and decreases the risk of a cyber attack. When

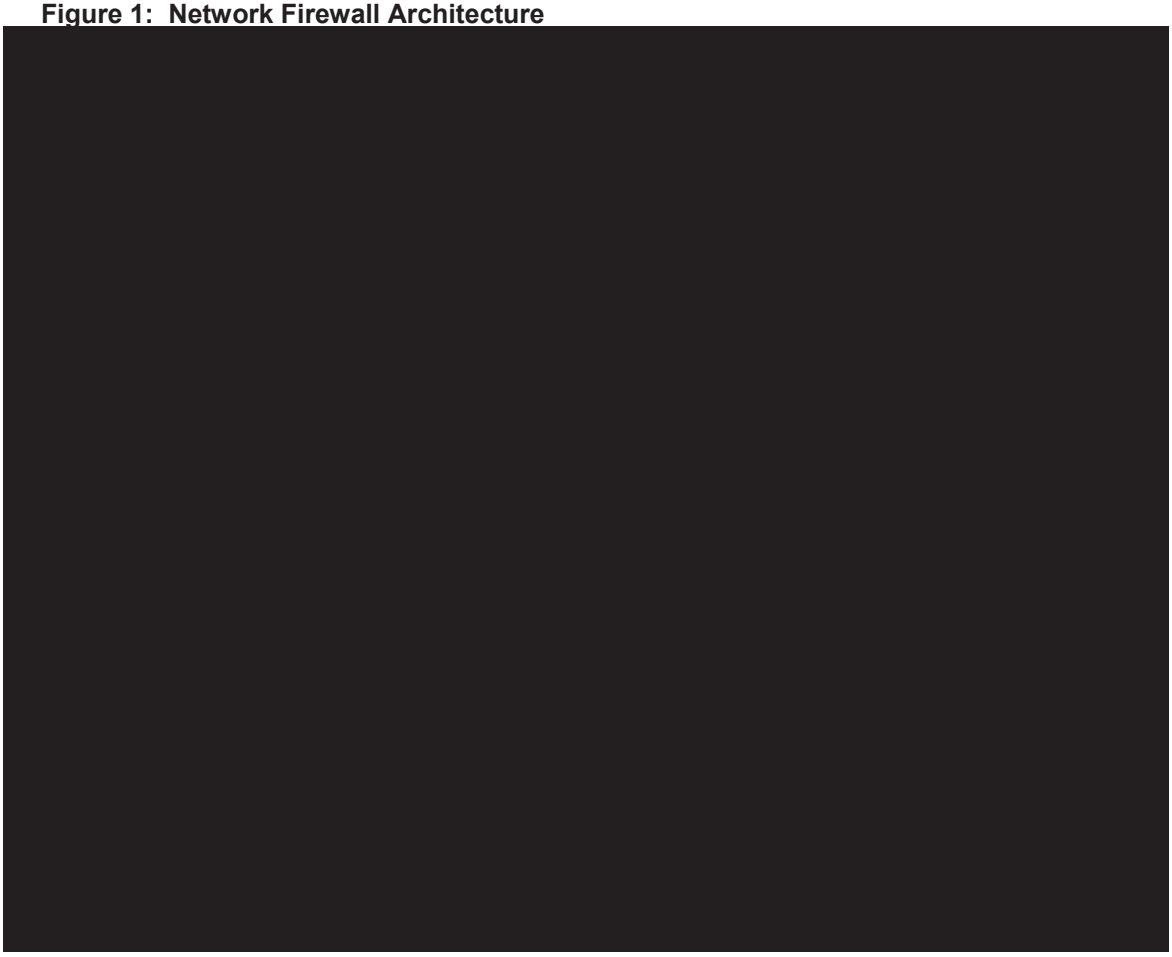
[21] NIST SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy* (September 2009).
[22] The FDIC has concluded that OMB Circular A-130, dated July 28, 2016, is generally applicable to the FDIC, and the FDIC should generally adhere to it, subject to certain caveats. These caveats include that: (a) the FDIC submits its budget to OMB for informational purposes, not approval; (b) the FDIC’s statutory mission or requirements take precedence when OMB’s instructions conflict with FDIC independence and supervisory authority; and (c) the Federal Information Technology Reform Act, one of the statutes in support of OMB’s authority under OMB Circular A-130, is not legally binding on the FDIC, although voluntary compliance can be considered.
[23] NIST Information Technology Lab Bulletin, *Protecting Information Systems with Firewalls: Revised Guidelines on Firewall Technologies and Policies* (October 2009).
[24] OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (October 2015) requires Federal agencies to employ defense-in-depth cybersecurity strategies. According to OMB, such strategies involve the layering of people, processes, technologies, and operations to achieve more secure Federal information systems.

organizations have a business need to allow a particular type of network traffic, they may create a firewall rule to allow the traffic. NIST SP 800-41 recommends that organizations review their firewall policies on a frequent basis to identify rules that are no longer needed. Firewalls are, therefore, only as effective as the rules that organizations define for them.

The FDIC deploys firewalls at both the perimeter and interior of its network. The perimeter firewalls control the flow of inbound and outbound traffic between the Internet and the internal network. The perimeter firewalls control inbound traffic through the use of "ingress" rules that inspect traffic and permit or deny requests for access to FDIC systems. Ingress rules help to prevent external cyber threats, such as malicious software known as malware, from entering the network. The perimeter firewalls also use "egress" rules to control outbound traffic. By controlling the type of traffic allowed to flow out of the network, the FDIC can prevent unwanted communication should a network IT device, such as a server, become compromised by an attacker or malware. This reduces the risk of unauthorized exfiltration of sensitive FDIC information.

The FDIC's interior firewalls provide an added layer of security against cyber threats. These firewalls operate within the network to monitor and block user access to unauthorized websites, such as gambling sites and pornographic sites. The interior firewalls also scan network traffic to identify and block malware that can damage or disable information systems and network IT devices. Figure 1 illustrates the architecture of the FDIC's perimeter and interior network firewalls.

Figure 1: Network Firewall Architecture



Within the FDIC, the Office of the Chief Information Security Officer (OCISO)—a component of the CIOO—has overall responsibility for the FDIC's information security program, including the network firewalls. Staff within the OCISO's Security Engineering Section serve as firewall administrators and manage the firewall operations. These firewall administrators oversee a firewall support team comprised of contractor personnel who perform the day-to-day administration of the firewalls. The OCISO staff and contractor personnel are responsible for managing the network firewalls in accordance with FDIC policy and guidelines; processing requests to add, change, or remove firewall rules; and maintaining firewall documentation, such as change requests, policies and procedures, and justifications for firewall rules.

Security Information and Event Management Tool

Preventive controls, such as firewalls, help organizations block attackers from gaining access to information systems and networks. Preventive controls alone, however, are not sufficient to mitigate the risk of cyber threats. Organizations must

also implement detective controls to monitor their information systems and networks for indications of cyber threats. A key goal of detective controls is to reduce the amount of time that an attacker can remain within a network. The longer an attacker remains within a network, the more opportunity the attacker would have to damage critical IT operations and information systems, or corrupt or steal sensitive data.

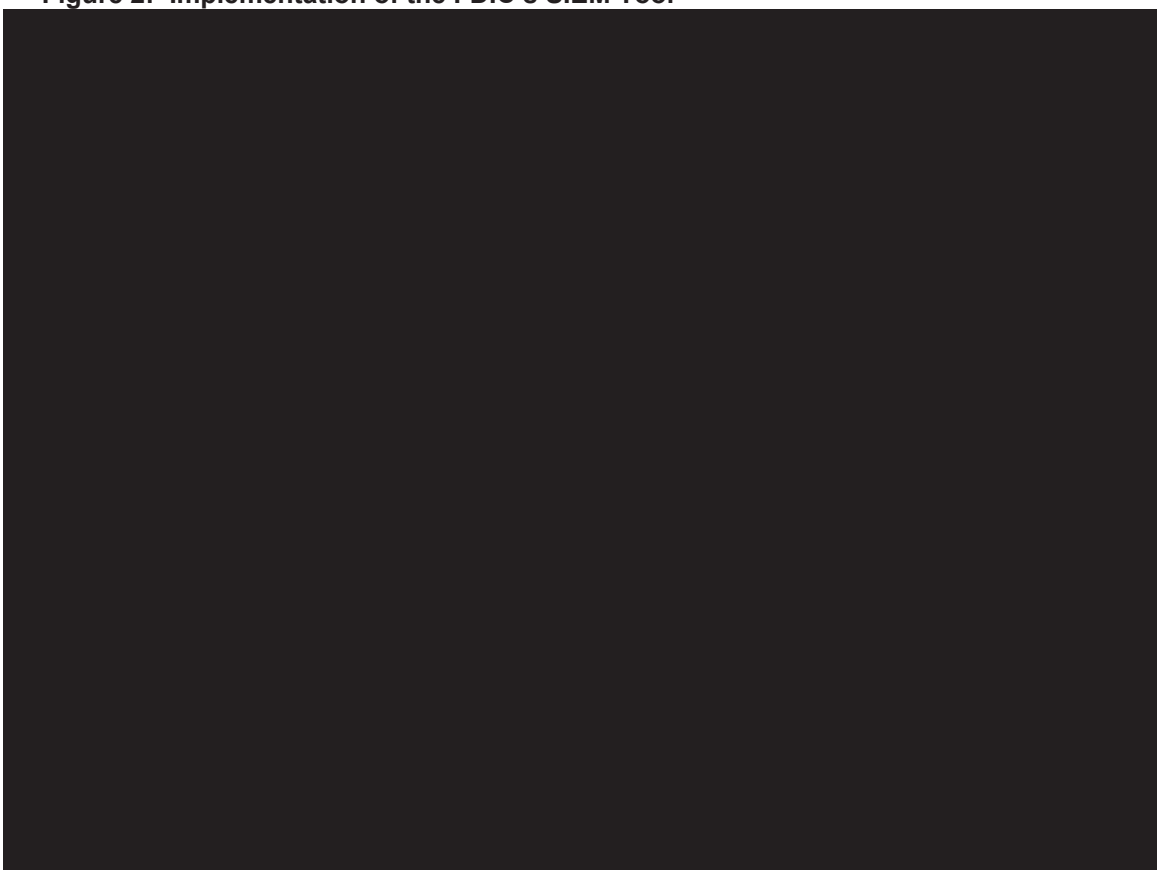
According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, dated September 2011, organizations can enhance their ability to identify inappropriate or unusual activity through the use of a SIEM tool.[25] SIEM tools collect vast amounts of audit log data generated by information systems and IT devices and analyze that data for indications of cyber threats. Audit logs are records of system activity (that is, machine-to-machine and human-to-machine events) that occurs within information systems and IT devices. Common system activities logged by organizations include successful and failed login attempts, account creations and deletions, the use of elevated privileges, and system startups and shut downs. According to NIST SP 800-92, *Guide to Computer Security Log Management*, routine analysis of audit log data can help organizations identify security incidents, policy violations, fraudulent activity, and operational problems.[26]

In January 2014, the FDIC implemented its current SIEM tool. The SIEM tool is one of several security solutions the FDIC uses to detect cyber threats on the network.[27] The SIEM tool collects audit log data from servers, routers, workstations, firewalls, and other network IT devices[28] and "aggregates" this data into a common repository and format for analysis. The SIEM tool then runs custom developed "Use Cases" against the audit log data to identify potential cyber threats. Use Cases are automated queries that organizations develop to identify specific types of events or patterns of activity that may indicate a cyber attack is occurring. At the time of our audit, the FDIC had developed [redacted] Use Cases and incorporated them into its SIEM tool. The FDIC designed these Use Cases to detect such activities as [redacted]

[25] NIST SP 800-137, *Information Security Continuous Monitoring (ICSM) for Federal Information Systems and Organizations* (September 2011).
[26] NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006).
[27] For example, the FDIC uses a third-party software product on its workstations and servers to detect and prevent viruses and malware, and [redacted].
[28] For the 30-day period ended October 26, 2017, audit log data collected by the SIEM tool contained an average of [redacted].

When a Use Case detects suspicious activity, the SIEM tool sends an alert to the FDIC's Computer Security Incident Response Team (CSIRT).[29] CSIRT, which is overseen by the OCISO, reviews the alerts to determine whether they warrant an investigation. Such investigations are designed to identify incidents with the potential to impact the security of the FDIC's information systems. Figure 2 illustrates how the FDIC has implemented the SIEM tool to detect cyber threats on its network.

Figure 2: Implementation of the FDIC's SIEM Tool



The OCISO's Security Engineering Section has primary responsibility for overseeing the implementation of the SIEM tool. The Security Engineering Section coordinates closely with CSIRT.

[29] CSIRT provides technical assistance to system administrators, monitors security vulnerabilities, and investigates incidents. CSIRT has responsibility for gathering and documenting pertinent information about incidents and forwarding the materials to appropriate FDIC management officials.

AUDIT RESULTS

We identified weaknesses that limited the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. With respect to the network firewalls, we found that:

- Many firewall rules lacked a documented justification, and the majority of firewall rules ([redacted]) were unnecessary. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure they continued to be needed.

- Firewalls did not comply with the FDIC's minimally acceptable system configuration requirements. In addition, the FDIC did not update its minimum requirements in a timely manner to address new security configuration recommendations approved by NIST.

- The FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls. In addition, [redacted]

- [redacted].

On February 9, 2018, we notified the CIO and then-Acting CISO of concerns regarding the administration of the network firewalls (see Appendix 5). The CIO and then-Acting CISO concurred with our concerns and stated that the CIOO was taking corrective actions (see Appendix 6). Weaknesses in the FDIC's network firewalls increased the risk of potential malicious activity, [redacted].

The FDIC properly set up its SIEM tool to collect audit log data from key network IT devices. In addition, the SIEM tool effectively formatted that data to allow for analysis of potential cyber threats. However, the FDIC did not have a written process for identifying, prioritizing, implementing, maintaining, and retiring Use Cases for the SIEM tool. In addition, [redacted] Use Cases used by the SIEM tool were [redacted]. These weaknesses reduced the FDIC's assurance that the SIEM tool was [redacted].

Firewall Rules Lacked Key Documentation

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*,[30] recommends that Federal agencies document each exception to the firewall policy with a supporting mission/business need and duration of that need. The FDIC creates firewall rules for such exceptions.

We selected nine egress rules in the network perimeter and interior firewalls and found that the CIOO had no documentation to support the mission/business need for each rule.[31] Specifically, the CIOO did not document who requested the nine rules, what mission/business needs supported the rules, the duration of the rules, or who had approved the rules for implementation. The then-Acting CISO explained that the FDIC had implemented the nine rules before March 2014, when the CIOO established a formal change request process requiring that new firewall rules be approved and documented with a supporting mission/business need.[32]

In response to our concerns about undocumented firewall rules, the CIO and CISO informed us that the OCISO completed a remediation effort in April 2018 to ensure the firewall rules were brought into compliance with the CIOO's current change request process.[33] Subsequently, on July 25, 2018, the CIO and CISO informed us that the OCISO had initiated, but not yet completed, a second review of all firewall rules to ensure they were accurately documented.

Unless firewall rules are supported by a documented mission/business need and an approval, FDIC management has no assurance that the access permitted by those rules is warranted. As described later, the lack of proper documentation for firewall rules limited the FDIC's ability to review firewall rules in order to determine whether they continued to serve a business need.

Recommendation

We recommend that the CIO:

(1) Require that all existing firewall rules be documented with an approval and mission/business need, including the duration of that need.

[30] NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* (April 2013) contains guidance relating to the security controls for Federal information systems.
[31] Our selection was judgmental; therefore, our results cannot be projected to the population. Appendix 1 contains additional information regarding how we selected the nine rules.
[32] FDIC, *Firewall Change Request Process*, Ver. 1.2 (originally issued March 2014 and revised April 2017).
[33] We did not assess the adequacy of this remediation effort.

Numerous Firewall Rules Were Unnecessary

NIST SPs 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*, and 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, recommend that Federal agencies:

- Establish an overall firewall policy that defines how the organization will handle its network traffic;
- Configure their firewalls to block all inbound and outbound network traffic that is not expressly permitted by the organization's firewall policy;
- Review firewall rules within an organization-defined frequency, and remove any rules that are no longer supported by an explicit mission/business need; and
- Conduct periodic "reviews"[34] of firewall rules by individuals who are not part of the firewall administration process.

On December 4, 2017, following our inquiry, an FDIC firewall administrator determined that eight of the nine sampled rules did not serve a current mission/business need and removed them.[35] In the same month, we advised the CIO and then-Acting CISO that there were likely additional firewall rules with no mission/business needs. Allowing unnecessary rules to exist in the network firewalls presents a security risk, [redacted]. We suggested that the CIOO review all network firewall rules to ensure that they were supported by a current mission/business need, and if not, remove them.

On May 8, 2018, OCISO staff represented that the firewall administrators had completed a review of the network firewall rules and removed [redacted].[36] The firewall administrators stated that the majority of rules removed had not been used within the prior 90-day period and were, therefore, considered unnecessary.

We identified three principal causes for the unnecessary firewall rules: (1) an inadequate firewall policy and supporting procedures; (2) ineffective processes for

[34] We use the term "review" so as to distinguish the NIST requirement from this present audit, and to clarify that the NIST reviews are not required to be conducted in accordance with Government Auditing Standards.
[35] The firewall administrator advised that the remaining firewall rule served a business need.
[36] We did not assess the adequacy of the OCISO's review, nor did we validate the number of rules reviewed or removed by the firewall administrators.

reviewing firewall rules; and (3) insufficient action to address prior security weaknesses.

Inadequate Firewall Policy and Procedures

NIST SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*, recommends that organizations establish a firewall policy that specifies how the organization's firewalls should handle inbound and outbound network traffic. According to NIST SP 800-41, the firewall policy should be documented in a system security plan and maintained and updated frequently as classes of new cyber attacks or vulnerabilities arise, or as the organization's needs change. Further, the firewall policy should address how changes in firewall rules are handled. NIST SP 800-41 adds that a firewall policy is an important control for reducing the risk of cyber attacks and decreasing the volume of traffic on an organization's network.

The FDIC's Data Communications general support system covers the network firewalls. According to OMB Circular A-130, Appendix III, a general support system is an interconnected set of information resources under the same direct management control that shares common functionality. The Data Communications general support system consists of firewalls, routers, and switches and other network devices that support FDIC activities and interface with the Internet, external systems and networks, and remote users.

We reviewed the security plan for the Data Communications general support system and found that it did not contain a firewall policy. The FDIC's security plan, however, referenced the FDIC's *ISPS Standards for Systems and Communications Protection* document (ISPS Standards Document). We found that the ISPS Standards Document was incomplete, even though it contained certain information recommended by NIST SP 800-41 for a firewall policy. For example, key sections of the ISPS Standards Document, such as roles and responsibilities, controls recommended by NIST, and processes for approving exceptions to the policy were blank. The ISPS Standards Document also referenced outdated OMB and FDIC policies. In addition, as of March 2018, FDIC management had not approved the ISPS Standards Document.

Further, in response to concerns we raised regarding the administration of the network firewalls, the OCISO performed an assessment to identify operational tasks supporting the firewalls that lacked supporting documentation. Based on the results of this assessment, the OCISO revised 8 of its 14 standard operating procedures (SOPs) supporting the management and operation of the network firewalls. The revisions addressed such things as how firewall change requests should be processed; how upgrades to the perimeter firewalls should be handled; and how

firewall rules should be updated when servers are removed from the network. The OCISO completed the revisions to the eight SOPs in May 2018. Further, the OCISO retired 1 of the 14 SOPs and created 5 new SOPs to address undocumented firewall support processes.

One of the five new SOPs defined how firewall administrators should conduct quarterly reviews of firewall rules. However, the SOP did not require firewall administrators to document these reviews. According to GAO's *Standards for Internal Control in the Federal Government,*[37] Federal agency management must document the results of its ongoing monitoring to identify internal control issues. The lack of documentation related to the review of firewall rules limited the FDIC's assurance that the reviews were being conducted properly and timely. It also limited the FDIC's assurance that firewall rules complied with the firewall policy, and that unnecessary rules were promptly identified and removed.

NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, states that policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government.[38] In addition, FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*,[39] emphasized the importance of policies and procedures as critical components of an effective internal control system. Without a current firewall policy and adequate supporting SOPs, employees and contractor personnel may not manage the network firewalls in a proper, consistent, and disciplined manner. [redacted]

Ineffective Processes for Reviewing Firewall Rules

NIST SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*, recommends that organizations review their firewall rules on a periodic basis. Doing so helps to ensure that firewall rules continue to comply with firewall policies and unnecessary rules are identified and removed. NIST SP 800-41 also recommends that organizations use automated tools whenever possible to facilitate these reviews. NIST notes that automated tools can be more effective than manual reviews in identifying rules that are redundant or inconsistent with security policies; flagging

[37] GAO Report, *Standards for Internal Control in the Federal Government* (GAO-14-704G) (September 2014).
[38] NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006). It is the FDIC's position that FIPS 200 is not binding on the Corporation because the Secretary of Commerce, who approved FIPS 200, does not have the authority to impose mandatory requirements on the FDIC. Nevertheless, the FDIC views the document as guidance for "best practices" in implementing security measures for information systems.
[39] FDIC, *Enterprise Risk Management Program* (April 2012). This circular was superseded on October 25, 2018 and renamed FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program.* This Directive also emphasizes the importance of policies and procedures as critical components of an effective internal control system.

rules that are no longer used; and helping to document business justifications for rules.

An FDIC firewall administrator advised us on October 18, 2017, that the firewall support team conducted manual reviews of the network firewall rules on a quarterly basis. However, the firewall support team did not use an automated tool to facilitate these reviews. The firewall administrator subsequently explained that the large number of rules in the network firewalls did not allow for the firewall support team to review the vast majority of rules each quarter. The firewall administrator advised that the firewall support team only had time to review about [redacted] firewall rules manually during each quarterly review – approximately [redacted] of the total number of firewall rules. This is a relatively small percentage, given that the population of rules during our review was [redacted]. In addition, the firewall support team did not document the quarterly firewall reviews because the OCISO had not established a requirement to do so. As a result, it was not possible to determine which rules the firewall support team reviewed, or when the team conducted the quarterly reviews.

Manually reviewing thousands of firewall rules is cumbersome and impractical, and placed a considerable burden on the firewall support team to ensure that the rules were still needed and properly configured. The manual reviews were especially difficult because there was no documentation regarding the mission/business need (including the duration), nor information about the request or approvals for many firewall rules. According to the firewall administrator, the lack of documentation required staff to research the historical record of who requested the rule and whether the rule was still needed. Such work was inefficient and time consuming.

In July 2011, the CIOO purchased an automated firewall tool to facilitate the administration of the network firewall rules. However, the firewall tool remained in a test environment until January 2018 – more than 6½ years later – and the firewall support team did not use the tool to administer the network firewalls. As a result, the FDIC received little value for the $73,578 it paid to purchase and maintain the firewall tool. It is not clear why the tool remained in a test environment for this length of time. We notified the CIO and then-Acting CISO of our concerns described above, and firewall administrators subsequently began testing new automated tools to administer the network firewalls. On April 12, 2018, the FDIC's Security and Enterprise Architecture Technical Advisory Board (SEATAB)[40] approved the procurement of a

[40] The FDIC established the SEATAB in 2018 to govern its Enterprise Architecture and implement its IT strategic direction through the development and adoption of technical guidance and standards. The SEATAB's respons bilities include, but are not limited to, evaluating and approving the introduction of all new IT at the FDIC. The SEATAB is comprised of representatives from the Division of Information Technology and the OCISO.

new firewall tool. The FDIC began using an evaluation/trial copy of a new firewall tool during the course of this audit; we did not review the adequacy of this tool.

Further, NIST SP 800-41 states that it is useful for organizations to have individuals who are not part of the organization's firewall policy and rule review team perform occasional reviews of firewall rules. These occasional reviews are separate and distinct from the regular reviews of firewall rules that firewall administrators perform, and, therefore, these reviews provide an outside view of the extent to which the firewall policy and rules comply with the organization's security goals. The CIOO did not conduct such reviews of its firewall rules because it had not established a requirement to do so.

Weaknesses in the FDIC's firewall review process allowed thousands of unnecessary firewall rules to go undetected for a lengthy period of time, including 8 of the 9 rules we reviewed. Due to the lack of documentation, we were not able to determine the duration of this weakness. This lapse increased the risk that [redacted].

Insufficient Action to Address Prior Security Weaknesses

[redacted]

[redacted]

[41] We did not assess the adequacy of these actions.

[redacted].

Interim Reporting on Firewall Weaknesses

On February 9, 2018, we notified the CIO and then-Acting CISO of our concerns regarding the administration of the network firewalls discussed in this report: (1) the lack of documentation and approvals for firewall rules; (2) an ineffective firewall review process; and (3) the lack of an automated tool to review firewall rules (see Appendix 5). On February 20, 2018, the CIO and then-Acting CISO indicated that the FDIC concurred with our concerns and described planned corrective actions (see Appendix 6). As of July 25, 2018, CIOO staff represented that they had either taken or planned to take the following actions by December 30, 2018 to strengthen the administration of the network firewalls:[42]

- Review all firewall rules and remove any rules that do not have a current mission/business need;
- Ensure that all remaining rules have a documented business justification and approval;
- Procure and begin implementing a new firewall tool to manage and review the network firewall rules; and
- Revise and establish new firewall SOPs.

Further, CIOO staff advised that they planned to [redacted] help identify unused firewall rules. In addition, OCISO staff planned to integrate its new firewall tool into the FDIC's [redacted]

Recommendations

We recommend that the CIO:

(2) Establish and implement a firewall policy consistent with NIST guidance.

[42] We did not assess the implementation of the FDIC's corrective actions, including whether the corrective actions were completed by December 30, 2018.
[redacted]

(3) Establish and implement a procedure to conduct reviews of firewall rules by individuals who are not part of the firewall administration process.

(4) Require that the quarterly reviews of firewall rules by firewall administrators be documented.

Firewalls Did Not Comply with Baseline Configurations

FISMA requires Federal information security programs to include policies and procedures for ensuring that agencies comply with their "minimally acceptable system configuration requirements." Agencies develop and record these requirements in a document or repository called a "baseline configuration." A baseline configuration is a set of specifications (for example, configuration settings, software versions, patch levels, and system documentation) for an information system that management has formally approved and can only be changed through a formal change control process. Agencies use baseline configurations as a frame of reference to assess their information systems for compliance with configuration requirements. Ensuring compliance with baseline configuration requirements is an important step towards properly securing Federal information systems.

CIOO Policy 16-005, *Policy on Secure Baseline Configuration Guides* (SBCG),[44] dated December 9, 2016, assigns responsibility to the OCISO for scanning FDIC information systems using an automated tool to determine whether the systems comply with applicable baseline configuration requirements. The OCISO provides the results of these scans to CIOO stakeholders who use the information to evaluate and address instances of noncompliance.

We found that the scan results completed on November 14, 2017, did not [redacted].[45] Because each firewall may be configured differently, it is critical that the FDIC subject each firewall to a regular scan.

Further, CIOO Policy 16-005 states that the baseline configuration settings for all FDIC IT products, applications, and operating systems (including the network firewalls) must comply with [redacted] of their associated baseline configuration requirements.[46] According to the scan results, the network perimeter and interior firewalls achieved average compliance of only [redacted] percent,

[44] FDIC CIOO Policy 16-005, *Policy on Secure Baseline Configuration Guides* (December 2016).
[45] See Appendix 1 for a description of the types of perimeter and interior firewalls the FDIC has deployed on its network.
[46] CIOO Policy 16-005 states that compliance is calculated by dividing the total number of information system security controls passed/met during the scan by the total number of security controls in the baseline configuration that were tested.

respectively, of their baseline configuration requirements. For example, firewall configurations did not [redacted].

The low compliance rate identified by the scan results meant that the network firewalls were at elevated risk to known security threats. Moreover, the volume of noncompliance exceeded the [redacted] tolerance level established by the FDIC in CIOO Policy 16-005.

After we brought the exceptions described above to the attention of CIOO representatives, they advised that, as of December 1, 2017, the primary and backup perimeter and interior firewalls had been scanned. Further, these firewalls had been brought into compliance with CIOO Policy 16-005. We confirmed that the scan results included all of the primary and backup perimeter and interior firewalls and reflected an average rate of compliance of [redacted] relative to their approved baseline configuration.

GAO, in its report entitled *Information Security, FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain*, noted that the FDIC had not consistently developed baseline configurations for its information systems.[47] Accordingly, GAO recommended that the FDIC establish and implement baseline configurations for its information systems. CIOO representatives advised that they had completed actions to address GAO's prior recommendation on December 1, 2017, and GAO subsequently closed the recommendation.

Baseline Configurations Were Outdated

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, recommends that agencies periodically review and update the baseline configurations for their information systems to ensure they remain current. In addition, CIOO Policy 16-005, and its implementing procedures in the *Secure Baseline Configurations Program* (*SBCG) Process and Procedures,* Version 4.0,[48] requires that CIOO staff review and update baseline configurations as system deviations are identified, and no less than annually.

To help agencies develop and maintain secure baseline configurations for their information systems, NIST developed the National Checklist Repository – a publicly

[47] GAO Report, *Information Security: FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain* (GAO-14-674) (July 2014).
[48] FDIC CIOO, *Secure Baseline Configurations Program Process and Procedures,* Version 4.0 (January 2017).

available resource containing security configuration checklists[49] for specific IT products or categories of IT products. NIST 800-70, Rev. 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, recommends that agencies use the security configuration checklists in the National Checklist Repository when configuring their information systems and applications.

[redacted].

Although CIOO Policy 16-005 requires CIOO staff to use the National Checklist Repository when developing baseline configurations, the policy does not require staff to check the repository on a regular basis for new or revised checklists. As a result, the FDIC's baseline configurations may not reflect the most current security configuration recommendations approved by NIST. [redacted].

Recommendation

We recommend that the CIO:

(5) Establish and implement a requirement to review the National Checklist Repository on a regular basis; update the FDIC's baseline configurations for network firewalls; and document the results of the review.

Controls Over Access to Local Firewall Accounts Were Ineffective

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, recommends that Federal information systems uniquely

[49] NIST SP 800-70, Rev. 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, February 2018, defines a security configuration checklist as a series of instructions or procedures for configuring an IT product to a particular operational environment; for verifying that the product has been configured properly; and/or for identifying unauthorized changes to the product.
[redacted]

identify and authenticate individuals and processes that access these systems.[52] Such access occurs through various types of accounts. Identification and authentication allow organizations to monitor an individual's activity within the information system, thereby promoting accountability and reducing the risk of misuse.

Identification and authentication are particularly important for administrative accounts within information systems. Administrative accounts have elevated access privileges that can be used to create other accounts, change configuration settings, or bypass system controls to perform troubleshooting activities. For these reasons, administrative accounts are highly sought-after targets by hackers and other adversaries who may wish to use the accounts to corrupt data, launch attacks, or conduct other malicious activities.

We judgmentally selected [redacted] firewalls on the network, to determine whether they required individuals and processes to uniquely identify and authenticate when using the firewall's local accounts (see text box). The FDIC's baseline configuration [redacted] states that except for [redacted]," individuals must uniquely identify and authenticate when they access the firewalls. As described below, the CIOO did not implement adequate controls to identify and authenticate administrators [redacted]

What is a local account?

Local accounts are different from network accounts. Local accounts control access to a single, physical IT device, such as a firewall. When an individual logs into the device using a local account, the IT device checks its own list of User IDs and passwords stored locally on the device to see if the individual is permitted access. This differs from a network account that uses a central security service, such as the Microsoft Active Directory (Active Directory), to identify and authenticate individuals.

[redacted]

[redacted]

[52] Identification is the process of uniquely identifying a user or process that accesses an information system. Authentication is the process of verifying the user or process is genuinely who or what they claim to be. For example, an information system may uniquely identify a user though his/her User ID and authenticate the user by checking that the supplied password is correct.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendations

We recommend that the CIO:

(6) Review all [redacted] firewalls and remove any local accounts that are not permitted by the approved baseline configuration.

(7) Perform a documented analysis to determine [redacted].

(8) Clarify policies and procedures to define [redacted] accounts that are required to be managed [redacted].

Restrictions on Access to Network Firewalls Were Inadequate

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, recommends that organizations implement the security principle of "least privilege."[53] NIST SP 800-53 also recommends that organizations prevent day-to-day users from having access to privileged IT functions. Further, CIOO Policy 14-005, *Policy on Restricting Administrative Access to both Servers and Workstations*, dated June 10, 2016, prohibits regular user accounts from having administrative rights on network IT resources.[54]

[53] The principle of "least privilege" refers to the security objective of restricting user access to only those IT resources needed to perform official duties.
[54] Although CIOO Policy 14-005 addresses servers and workstations, CIOO staff stated that this policy also applies to IT infrastructure components, including the network firewalls.

The FDIC assigns certain CIOO network users an additional administrative account to perform systems maintenance and other types of necessary IT troubleshooting. As previously stated, hackers and other adversaries target administrative accounts because of their elevated privileges. According to CIOO Policy 14-005, a compromise of an administrative account would pose a significant risk to the FDIC's environment. As a result, the CIOO grants administrative accounts on a limited basis. Because of their importance, the FDIC subjects administrative accounts to enhanced monitoring and additional security controls. For these reasons, regular network user accounts, which are not subject to enhanced monitoring and additional security controls, should not be granted elevated privileges to perform administrative functions.

The CIOO uses [redacted]

[redacted].

Process for Managing SIEM Tool Use Cases Needed Improvement

As discussed earlier in this report, the FDIC has deployed a number of security solutions designed to detect cyber threats on its network. One such solution is the SIEM tool. [redacted].

The FDIC periodically adds new Use Cases in the SIEM tool to address *vulnerabilities* and *common threats*. The FDIC identifies vulnerabilities through [redacted].

According to Gartner, Inc.,[57] "a structured process to identify, prioritize, implement and maintain Use Cases allows technical professionals to align monitoring efforts to security strategy, choose best-fit solutions and maximize the value of security monitoring tools."[58] In addition, Gartner, Inc. recommends that "technical professionals focused on security monitoring and operations implement a process to frequently review and tune (and eventually retire) Use Cases to adjust to changes in the IT environment, the business and the threat landscape."[59]

Based on our industry research, including Gartner's research, we developed Figure 3 below which illustrates how a structured process for managing Use Cases could be implemented at the FDIC. This process would help to ensure that Use Cases remain effective in detecting cyber threats as changes occur in an organization's specific IT and business environments and the cyber threat landscape. However, the OCISO did not establish a written process to manage Use Cases in the SIEM tool because doing so was not a priority.

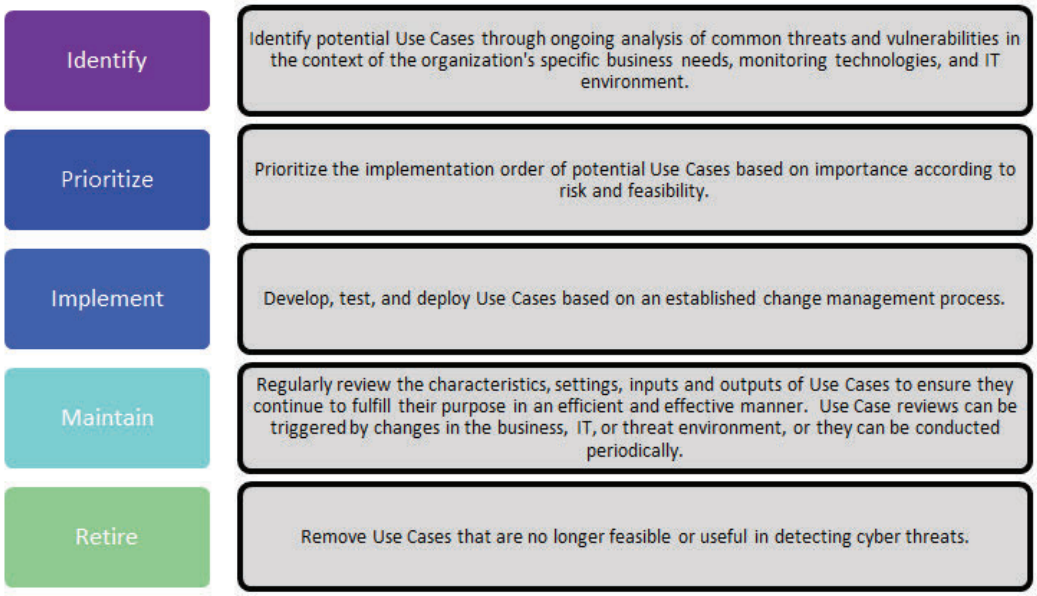
[redacted].

[57] Gartner, Inc. is a global research and advisory firm that provides insights, advice, and tools for leaders in IT, and other enterprise functions.

[58] Gartner, Inc., *How to Develop and Maintain Security Monitoring Use Cases* (January 2018), 1.

[59] Gartner, Inc., *How to Develop and Maintain Security Monitoring Use Cases*, 2.

Figure 3: Use Case Management Process



Source: OIG analysis of industry research related to Use Case management.

Vulnerabilities

[redacted]

[redacted].

[60] Gartner, Inc., *How to Develop and Maintain Security Monitoring Use Cases*, 7.

CSIRT representatives stated that the Use Cases recommended in the After Action Report did not constitute formal actions that needed to be taken. Instead, the OCISO implemented recommended Use Cases if it determined they were warranted in light of the FDIC's other security monitoring activities. As a result, OCISO did not establish formal due dates for the recommendations in the After Action Report or track them to completion. In addition, OCISO did not develop a written procedure to address corrective actions based on the results of its [redacted]. As a result, the FDIC may not develop important Use Cases identified through [redacted].

Common Threats

Organizations should consider common threats when identifying potential Use Cases. Further, organizations should consider common threats in the context of the organization's specific IT and threat environment, business activities, and existing monitoring technologies. Such an approach helps to ensure that organizations identify Use Cases that are most relevant to the organization.

[redacted]. As a result, the FDIC cannot be sure that it is identifying all relevant Use Cases for the FDIC's IT environment.

Further, establishing a written process for managing Use Cases that defines key roles and responsibilities would help ensure a disciplined and repeatable approach. It would also provide a means for the FDIC to retain organizational knowledge and mitigate the risk of that knowledge being limited to a few personnel who could depart the FDIC. In addition, a written process would allow the FDIC to monitor and evaluate the management of Use Cases for the SIEM tool, and communicate expectations to those responsible for the performance of this activity. Moreover, a written process would be consistent with GAO's *Standards for Internal Control in the Federal Government*, dated September 2014, which states that the effective design,

[redacted]

implementation, and operating effectiveness of an entity's internal control system requires appropriate documentation.

Recommendation

We recommend that the CIO:

(9) Document, approve, and implement a structured process for identifying, developing, prioritizing, deploying, maintaining, and retiring Use Cases for the SIEM tool.

Certain SIEM Tool Use Cases Did [redacted]

According to our analysis of industry research, organizations should implement a process to review and adjust Use Cases on a periodic basis to address changes in the IT environment. Changes in the IT environment require Use Cases to be updated regularly, so that they continue to address the threats they were intended to detect.

We tested all [redacted] Use Cases used by the SIEM tool and found that [redacted] did not flag the cyber threats they were intended to detect:

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted].

Recommendation

We recommend that the CIO:

(10) Document, approve, and implement a process to test and update Use Cases periodically in order to ensure they operate as intended.

FDIC COMMENTS AND OIG EVALUATION

The CIO Organization provided a written response, dated April 15, 2019, to a draft of this report. The response is presented in its entirety in Appendix 7. The CIO Organization concurred with all 10 of the report's recommendations.

Following the issuance of the draft report, the CIO Organization provided us with corrective action documentation for 8 of the 10 recommendations. We determined that the documentation was responsive for four of the eight recommendations and closed them. We plan to review the corrective action documentation for the other four recommendations as part of our audit follow-up process. The CIO Organization plans to complete corrective actions for the report's remaining two recommendations by January 31, 2020.

The report's six open recommendations will remain open until we confirm that corrective actions have been completed and are responsive. Appendix 8 contains a summary of the FDIC's corrective actions.

[62] The OCISO was not able to identify the configuration change that caused the Field Name to change.

Objective

The audit objective was to assess the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. We engaged Cotton and Company LLP (C&C) to perform the majority of audit planning and field work. We also consulted with C&C in preparing this audit report.

We conducted this performance audit from February 2017 to February 2019 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 2018. After March 2018, C&C and the OIG conducted certain follow-up interviews with representatives of the CIOO and gathered additional information related to the findings in this report.

Scope and Methodology

With respect to the network firewalls, the scope of the audit covered the [redacted] firewall devices deployed at the perimeter and interior, respectively, of the FDIC's network. At the time of our audit, the FDIC maintained a total of [redacted]

[redacted]

[redacted].

To assess the effectiveness of the network firewalls, we evaluated the FDIC's controls for justifying, reviewing, and approving firewall rules; establishing and ensuring compliance with baseline configuration requirements; and controlling access to firewall devices. As part of our work, we obtained and analyzed electronic copies of firewall rulesets from the OCISO for the [redacted] firewalls on the network as of September 7, 2017. We did not analyze the firewall rulesets for the [redacted] firewalls because these devices contained the same rules as the [redacted] firewalls.

We also obtained and analyzed electronic copies of firewall rulesets from the OCISO [redacted] as of September 7, 2017. We judgmentally selected these [redacted] firewall devices in a manner to achieve representation across FDIC Regional Offices. Collectively, the [redacted] firewall devices ([redacted]) that we reviewed contained a population of [redacted] firewall rules.

We judgmentally selected [redacted] rules and [redacted] rule from the population of [redacted] rules to determine whether the nine rules supported a current FDIC mission/business need. [redacted]. Judgmental samples are non-statistical and cannot be projected to the population. We determined that the population of firewall rules and configuration settings provided by the OCISO were sufficiently reliable for purposes of our testing by meeting with the firewall administrator and observing the process for generating the population of rules for each of the firewall devices we selected.

Our assessment of the network firewalls included discussions with OCISO managers and firewall administrators who had responsibility for managing and configuring the firewalls. In addition, we reviewed relevant security and systems documentation, such as the:

- FDIC Network Diagram (Version 9.4 2, dated July 2017);
- Data Communications System Security Plan, Version 4.0; and
- Secure Baseline Configuration Guide for perimeter and interior firewalls.

Further, we assessed the extent to which the CIOO addressed security weaknesses and recommendations related to the network firewalls in prior assessments conducted on behalf of the FDIC.

To assess the effectiveness of FDIC's SIEM tool, we:

- Determined whether key network IT devices provided the SIEM tool with audit log data for analysis;
- Assessed whether the SIEM tool effectively formatted audit log data to allow for subsequent analysis of potential cyber threats;
- Tested all [redacted] Use Cases in the SIEM tool to determine whether they operated as intended (that is, identified the suspicious activity the Use Cases were designed to detect and generated an associated alert); and
- Evaluated the FDIC processes for identifying, prioritizing, developing, deploying, maintaining, and retiring Use Cases to address changes in the FDIC's IT and cyber threat environment.

Our work related to the SIEM tool included discussions with OCISO managers, administrators, and CSIRT personnel who had responsibility for overseeing, administering, and using the SIEM tool. In addition, we reviewed relevant security and systems documentation, such as Use Cases, firewall alerts, and a listing of network assets reporting to the SIEM tool. Further, we reviewed relevant industry information, including research performed by Gartner, related to the use of the SIEM tool.

Regarding compliance with laws and regulations, we used relevant provisions of FISMA, government-wide information security policies and guidance, and FDIC policies, procedures, and guidance as criteria. These included:

OMB Policy

- Circular Number A-130, *Managing Information as a Strategic Resource*
- *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- Memorandum M-17-05, *Fiscal Year 2016 – 2017 Guidance on Federal Information Security and Privacy Management Requirements*

NIST Standards and Guidance

- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*
- SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

- SP 800-70, Rev. 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*
- 800-92, *Guide to Computer Security Log Management*
- SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- Information Technology Lab Bulletin, *Protecting Information Systems with Firewalls: Revised Guidelines on Firewall Technologies and Policies*

FDIC Policies, Standards, and Guidance

- *ISPS Standards for Systems and Communications Protection*
- Policy 14-005, *Policy on Restricting Administrative Access to both Servers and Workstations*
- Policy 16-005, *Policy on Secure Baseline Configuration Guides*
- *Secure Baseline Configuration Guide Process and Procedures*, Version 4.0

We assessed the risk of fraud and abuse related to our audit objective in the course of evaluating audit evidence. We performed our work at the FDIC's Virginia Square offices in Arlington, Virginia.

Glossary

Term	Definition
Advanced Persistent Threat	An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (for example, cyber, physical, and deception). These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. [NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*]
Audit Log	A chronological record of system activities, including records of system accesses and operations performed in a given period. [NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*]
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. [NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and* Organizations]
Component-Level Security	Security for subsystems of an information system. A subsystem is a major subdivision of an information system consisting of information, IT, and personnel that performs one or more specific functions. Examples of components of an information system include applications, networks, servers, or workstations. [NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*]
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*]
Cyber Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST SP 800-150, *Guide to Cyber Threat Information Sharing*]
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations. [Based on NIST SP 800-33, *Underlying Technical Models for Information Technology Security*]
[redacted]	[redacted]

Host	Almost any kind of computer, including a centralized mainframe that is a host to its terminals, a server that is host to its clients, or a desktop personal computer that is host to its peripherals. In network architectures, a client station (user's machine) is also considered a host because it is a source of information to the network, in contrast to a device, such as a router or switch that directs traffic. [NIST SP 800-44, Ver. 2, *Guidelines on Securing Public Web Servers*]
[redacted]	[redacted]
Insider Threat	A threat posed to the FDIC or U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any United States Government resource. This threat can include damage through espionage, terrorism, sabotage, unauthorized disclosure of classified information or unclassified sensitive information, or through the loss or degradation of FDIC resources or capabilities. [FDIC Circular 1600.7, *FDIC Insider Threat and Counterintelligence Program*]
Internet Protocol	The Internet Protocol controls the transfer of information from one device to another over the Internet through the management of specific, unique network addresses. [NIST ITL Bulletin, *Internet Protocol Version 6 (IPv6): NIST Guidelines Help Organizations Manage the Secure Deployment of the New Network Protocol*]
IT Strategic Plan	The FDIC's 2017-2020 Information Technology Strategic Plan identifies opportunities for the FDIC to improve internal operations in a world of ever changing technology. The plan identifies five major goals with supporting objectives designed to improve business capabilities and systems: (1) improve information security and privacy, (2) continuity of operations, (3) enterprise mobility, (4) information management and analytics, and (5) IT service delivery. [FDIC *Information Technology Strategic Plan* 2017 – 2020]
Malicious Code	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*]
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. [NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*]
National Institute of Standards and Technology	A non-regulatory agency of the U.S. Department of Commerce that promotes and maintains measurement standards and issues standards, guidelines, and publications to assist Federal agencies in implementing the FISMA. [NIST *Framework for Improving Critical Infrastructure Cybersecurity*]

Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual. [OMB Circular A-130]
Phishing Attack	A form of digital social engineering where attackers attempt to steal information such as credit card numbers, Social Security Numbers, User IDs, and passwords. Phishing uses authentic-looking emails to request information or direct users to a bogus website to collect information. [NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*]
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*]

Acronyms and Abbreviations

Active Directory	Microsoft Active Directory
AOR	Acceptance of Risk
APT	Advanced Persistent Threat
C&C	Cotton and Company, LLP
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
[redacted]	[redacted]
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
[redacted]	[redacted]
IP	Internet Protocol
ISPS Standards Document	ISPS Standards for Systems and Communications Protection Document
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	Personally Identifiable Information
SBCG	Secure Baseline Configuration Guide
SEATAB	Security and Enterprise Architecture Technical Advisory Board
SIEM	Security Information and Event Management
SOP	Standard Operating Procedure
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

Nature of Assessment	Summary of Findings and Recommendations
[redacted]	[redacted] The consulting firm categorized its findings and recommendations as Critical, Very Important, and Important.
[redacted]	[redacted] The consulting firm categorized its findings and recommendations as High, Medium, Low, and Informational.

Nature of Assessment	Summary of Findings and Recommendations
[redacted]	[redacted]
[redacted]	[redacted]

Office of Inspector General

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

Date: February 9, 2018

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

Noreen C. Padilla
Acting Chief Information Security Officer

/Signed/

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

Subject **Advisory Memorandum** | *Administration of Network Firewalls* | Assignment No. 2017-012

While conducting our ongoing audit of *Controls for Preventing and Detecting Advanced Cyber Threats*, we identified concerns regarding the administration of the FDIC's network firewalls that warrant your immediate attention. We initially advised you of similar concerns on December 5, 2017.

Background

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 exactly what network traffic is permitted.

The National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, recommends that federal agencies:

- configure firewalls in a manner so as to block all inbound and outbound network traffic that is not expressly permitted by the organization's firewall policy.
- subject firewall rules to a formal change management control process because they have the potential to impact the organization's security and business operations.
- document comments that describe each firewall rule.
- review firewall rules periodically to ensure continued compliance with established security policies. Doing so can identify rules that are no longer needed.

The FDIC Chief Information Officer (CIO) Organization has also defined firewall standards and procedures in the *ISPS Standards for Systems and Communications Protection* document, dated August 2016. These standards state that firewall rules must follow a formal change management process that includes management approvals. Such a process can help ensure

[redacted]

that firewall rules are properly justified and authorized. CIO Organization staff informed us that they began implementing a formal change management process for firewall rules in 2013.

The *ISPS Standards for Systems and Communications Protection* also state that firewall rules must be supported by a documented mission or business need, including the duration of that need. Such documentation serves to explain decisions to create firewall rules and accept the risk associated with the access they permit. In addition, the standards state that firewall rules must be reviewed on a quarterly basis, and any rules for which an explicit mission or business need no longer exists must be removed.

OIG Concerns

The OIG raises three primary concerns regarding the administration of the FDIC's network firewalls.

Lack of Documentation for Firewall Rules

The FDIC's network [redacted] (as of September 7, 2017). Based upon our audit work thus far, we have noted that the FDIC has not properly documented a number of its firewall rules with supporting explanations of the associated business need, nor has the FDIC documented approvals for these firewall rules.

In November 2017, we reviewed a sample of nine outbound rules in the [redacted] firewalls and requested business justifications. On December 4, 2017, an FDIC firewall administrator advised he determined that eight of these rules did not serve a current business need and, therefore, he disabled the eight rules. Two days later, the Acting Chief Information Security Officer (CISO) advised that the rules we inquired about were implemented before the CIO Organization established a formal process for firewall rules. As a result, the CIO Organization did not have any documentation as to who requested the rules, what business needs supported the rules, or who approved the rules for implementation.

On January 26, 2018, the Acting CISO advised that the FDIC had identified a large number of rules that did not have a documented business justification and/or had not been used recently. The lack of proper documentation limits the FDIC's ability to review firewall rules effectively to determine whether they continue to serve a business need.

Manual Review of Firewall Rules

[redacted]

2

[redacted]

allowed unnecessary firewall rules to go undetected, thus increasing the [redacted]

Lack of an Automated Tool to Review Firewall Rules

There are a number of automated tools available to facilitate the review of firewall rulesets. Such tools can be used to identify rules that are redundant or inconsistent with security policies, flag rules that are no longer used, and help document justifications for rules.

On January 26, 2018, the Acting CISO advised that the FDIC firewall administrators had implemented an automated firewall tool [redacted] earlier in the month to analyze the firewall ruleset. The CIO Organization originally purchased the [redacted] tool in July 2011; however, the tool remained in a test environment until January 2018. As a result, the FDIC has received little value for the licensing fees it has paid for the [redacted] tool since 2011. Further, firewall administrators have determined that the functionality of the [redacted] tool does not meet their needs. Therefore, FDIC firewall administrators are evaluating other tools for the FDIC environment.

Conclusion

[redacted]

We request that you provide us with a written response describing the actions the CIO Organization plans to take to address the risks described above, along with the timeframes for completing those actions. Please submit your response by February 16, 2018. We plan to continue our audit and will address any corrective actions taken by the CIO Organization in our written audit report.

If you would like to discuss these concerns further, please contact me at (703) 562-6316, or Joe Nelson, IT Audit Manager, (703) 562-6314.

cc: Rack D. Campbell, CIO Organization
Barbara A. Ryan, Deputy to the Chairman and Chief Operating Officer/Chief of Staff

3

[redacted]

FDIC

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

DATE: February 20, 2018

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

FROM: Howard G. Whyte [redacted]
Chief Information Officer and Chief Privacy Officer

Noreen C. Padilla [redacted]
Acting Chief Information Security Officer

SUBJECT: Management Response to the Advisory Memorandum Entitled *Administration of Network Firewalls* (Assignment No. 2017-012)

Thank you for the opportunity to provide a written response to the Office of Inspector General's (OIG) Advisory Memorandum on the *Administration of Network Firewalls*, issued February 9, 2018. In its memorandum, the OIG documented three primary concerns regarding the administration of the FDIC's network firewalls. We have carefully considered and concur with the identified issues.

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

We appreciate your staff's time and effort and we expect that the actions taken in response to this advisory memorandum will further enhance the FDIC's network firewall controls and reduce risk to the agency. Cybersecurity is essential in protecting the FDIC's data and systems and it remains a top priority.

MANAGEMENT RESPONSE

Advisory Area 1 – Lack of Documentation for Firewall Rules

The FDIC's [redacted] (as of September 7, 2017). FDIC has not properly documented a number of its firewall rules with supporting explanations of the associated business need, nor has the FDIC documented approvals for these firewall rules. In November 2017, OIG reviewed a sample of nine outbound rules in the [redacted] firewalls and requested business justifications. On December 4, 2017, an FDIC firewall administrator advised he determined that eight of these rules did not serve a current business need and, therefore, he disabled the eight rules. Two days later, the Acting Chief Information Security Officer (CISO) advised that the rules we inquired about were implemented before the CIO Organization established a formal process for firewall rules. As a result, the CIO Organization did not have any documentation as to who requested the rules, what business needs supported the rules, or who approved the rules for implementation. On January 26, 2018, the Acting CISO advised that the FDIC had identified a large number of rules that did not have a documented business justification and/or had not been used recently. The lack of proper documentation limits the FDIC's ability to review firewall rules effectively to determine whether they continue to serve a business need.

Management Decision: Concur

Corrective Action:
[redacted] The OCISO has begun a remediation effort to remove the unused rules and ensure undocumented rules are updated to match the current standard (defined in the Firewall Change Request Process v2.0 document). The scope of this review includes both the [redacted] firewalls. Status reports are provided to OCISO management on a weekly basis.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
The process of requiring business justification on new rules has been in place since 2013.
[redacted]

Estimated Completion Date: March 31, 2018

2

Advisory Area 2 – Manual Review of Firewall Rules

FDIC firewall administrators advised that they manually review firewall rules. However, these reviews are not documented. Manually reviewing thousands of rules is cumbersome and impractical, and places a considerable burden on firewall administrators to ensure that the rules are still needed and properly configured. A firewall administrator advised that the firewall team only has time to manually review a relatively small portion of the network firewall ruleset each quarter. The manual reviews were complicated by the lack of documentation for many firewall rules. Without documentation, firewall administrators must, in many instances, research who requested the rule and the basis for the request. Weaknesses in the firewall review process allowed unnecessary firewall rules to go undetected, thus increasing the risk that [redacted].

Management Decision: Concur

Corrective Action:

[redacted]. Standard Operating Procedures will be created to address all process changes. Additionally, the OCISO has obtained business analyst support to assist in identifying any operational tasks that lack supporting documentation. The status of this effort is reported to CIOO executive management in the CIOO weekly management report.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

[redacted]

Estimated Completion Date:

- Complete business analysis assessment: February 28, 2018
- Remove unused/redundant/shadow rules: March 31, 2018
- Ensure rules have associated [redacted] change numbers: March 31, 2018

3

- [redacted]
- [redacted]
- Update/Create Standard Operating Procedures: On-going

Advisory Area 3 – Lack of an Automated Tool to Review Firewall Rules.

There are a number of automated tools available to facilitate the review of firewall rulesets. Such tools can be used to identify rules that are redundant or inconsistent with security policies; flag rules that are no longer used, and help document justifications for rules. On January 26, 2018, the Acting CISO advised that the FDIC firewall administrators had implemented an automated firewall tool [redacted] earlier in the month to analyze the firewall ruleset. The CIO Organization originally purchased the [redacted] tool in July 2011; however, the tool remained in a test environment until January 2018. As a result, the FDIC has received little value for the licensing fees it has paid for the [redacted] tool since 2011. Further, firewall administrators have determined that the functionality of the [redacted] tool does not meet their needs. Therefore, FDIC firewall administrators are evaluating other tools for the FDIC environment.

Management Decision: Concur

Corrective Action:
The OCISO has evaluated and selected the [redacted] to support this requirement. [redacted]. The OCISO is in the process of procuring the product.

The [redacted] will be used to automate significant pieces of the firewall rule review process. Specifically, it will automate reporting of unused and redundant rules, and alerting when rules are added [redacted] will also be integrated with [redacted] to streamline and gain efficiencies in workflow processing of the rule reviews.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
The OCISO is leveraging the results identified during the evaluation period. The [redacted] is in procurement, and is scheduled to be deployed in production in Q2 2018.

Estimated Completion Date: June 30, 2018

Any questions regarding this response should be directed to Rack Campbell at (703) 516-1422) or Kim Farrell at (703) 516-5101.

cc: Susan E. H. Koepp, Acting Deputy Director, DOF, Corporate Management Control Branch
Russell G. Pittman, Director, DIT
Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Rack D. Campbell, Chief, DIT, Audit and Internal Control Section

4

FDIC

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

DATE: April 19, 2018

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

FROM: Howard G. Whyte [redacted]
Chief Information Officer and Chief Privacy Officer

Zachary Brown [redacted]
Chief Information Security Officer

SUBJECT: Advisory Memorandum Entitled *Administration of Network Firewalls* (Assignment No. 2017-012) - Progress Update

Thank you for the opportunity to provide a progress update on the status of the corrective actions included in the management's response to the Office of Inspector General's (OIG) Advisory Memorandum on the *Administration of Network Firewalls*, issued February 9, 2018. In its memorandum, the OIG documented three primary concerns regarding the administration of the FDIC's network firewalls.

Our response provides a description of the progress the Chief Information Officer (CIO) Organization has made to address the risks described in the OIG's memorandum including the timeframes for completing those actions. Our response is organized by the areas of concern raised by the OIG and contains actions planned or in process and the current status as of April 19, 2018.

We appreciate your staff's time and effort and we expect that the actions taken in response to this advisory memorandum will further enhance the FDIC's network firewall controls and reduce risk to the agency. Cybersecurity is essential in protecting the FDIC's data and systems and it remains a top priority.

MANAGEMENT RESPONSE

Advisory Area 1 – Lack of Documentation for Firewall Rules

The FDIC's network [redacted] (as of September 7, 2017). FDIC has not properly documented a number of its firewall rules with supporting explanations of the associated business need, nor has the FDIC documented approvals for these firewall rules. In November 2017, OIG reviewed a sample of nine outbound rules in the [redacted] firewalls and requested business justifications. On December 4, 2017, an FDIC firewall administrator advised he determined that eight of these rules did not serve a current business need and, therefore, he disabled the eight rules. Two days later, the Acting Chief Information Security Officer (CISO) advised that the rules we inquired about were implemented before the CIO Organization established a formal process for firewall rules. As a result, the CIO Organization did not have any documentation as to who requested the rules, what business needs supported the rules, or who approved the rules for implementation. On January 26, 2018, the Acting CISO advised that the FDIC had identified a large number of rules that did not have a documented business justification and/or had not been used recently. The lack of proper documentation limits the FDIC's ability to review firewall rules effectively to determine whether they continue to serve a business need.

Management Decision: Concur

Corrective Action:
[redacted] The OCISO has begun a remediation effort to remove the unused rules and ensure undocumented rules are updated to match the current standard (defined in the Firewall Change Request Process v2.0 document). The scope of this review includes both the [redacted] firewalls. Status reports are provided to OCISO management on a weekly basis.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
The process of requiring business justification on new rules has been in place since 2013. [redacted]

Estimated Completion Date: March 31, 2018

Status as of April 19, 2018:
The manual review of both the [redacted] firewall rules was completed on schedule. OCISO removed unused rules and validated the remaining rules were consistent with the current configuration standard, as defined in the Firewall Change Request Process v2.0. The final status report was provided to the Acting CISO on April 2, 2018.

2

Advisory Area 2 – Manual Review of Firewall Rules

FDIC firewall administrators advised that they manually review firewall rules. However, these reviews are not documented. Manually reviewing thousands of rules is cumbersome and impractical, and places a considerable burden on firewall administrators to ensure that the rules are still needed and properly configured. A firewall administrator advised that the firewall team only has time to manually review a relatively small portion of the network firewall ruleset each quarter. The manual reviews were complicated by the lack of documentation for many firewall rules. Without documentation, firewall administrators must, in many instances, research who requested the rule and the basis for the request. Weaknesses in the firewall review process allowed unnecessary firewall rules to go undetected, thus increasing the risk that the [redacted].

Management Decision: Concur

Corrective Action:

[redacted]. Standard Operating Procedures will be created to address all process changes. Additionally, the OCISO has obtained business analyst support to assist in identifying any operational tasks that lack supporting documentation. The status of this effort is reported to CIOO executive management in the CIOO weekly management report.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:

[redacted]

Estimated Completion Date:

- Complete business analysis assessment: February 28, 2018
- Remove unused/redundant/shadow rules: March 31, 2018
- Ensure rules have associated [redacted] change numbers: March 31, 2018

3

- [redacted]
- [redacted]
- Update/Create Standard Operating Procedures: On-going

Status as of April 19, 2018:
The business analyst assessment performed to identify any operational tasks that lack supporting documentation was completed on schedule and delivered to the Acting CISO on February 16, 2018. The assessment identified eight out of fourteen SOPs requiring revision and four new SOPs that should be drafted to document recurring work. Work to update and create Firewall Support SOPs is ongoing.
The manual review of firewall rules to identify rulesets that were redundant, inconsistent with the current configuration standard, or no longer used was completed on schedule. The [redacted] being implemented to automate the reporting of unused policies was reviewed and approved at the April 12, 2018 meeting of the Security and Enterprise Architecture Technical Advisory Board (SEATAB), and the procurement is complete.

Advisory Area 3 – Lack of an Automated Tool to Review Firewall Rules.

There are a number of automated tools available to facilitate the review of firewall rulesets. Such tools can be used to identify rules that are redundant or inconsistent with security policies; flag rules that are no longer used, and help document justifications for rules. On January 26, 2018, the Acting CISO advised that the FDIC firewall administrators had implemented an automated firewall tool [redacted] earlier in the month to analyze the firewall ruleset. The CIO Organization originally purchased the [redacted] tool in July 2011; however, the tool remained in a test environment until January 2018. As a result, the FDIC has received little value for the licensing fees it has paid for the [redacted] tool since 2011. Further, firewall administrators have determined that the functionality of the [redacted] tool does not meet their needs. Therefore, FDIC firewall administrators are evaluating other tools for the FDIC environment.

Management Decision: Concur

Corrective Action:
The OCISO has evaluated and selected the [redacted] to support this requirement. [redacted]. The OCISO is in the process of procuring the product.

The [redacted] will be used to automate significant pieces of the firewall rule review process. Specifically, it will automate reporting of unused and redundant rules, and alerting when rules are added [redacted] will also be integrated with [redacted] to streamline and gain efficiencies in workflow processing of the rule reviews.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
The OCISO is leveraging the results identified during the evaluation period. The [redacted] is in procurement, and is scheduled to be deployed in production in Q2 2018.

4

Estimated Completion Date: June 30, 2018

Status as of April 19, 2018:
The [redacted] was reviewed and approved during the SEATAB meeting held on the April 12, 2018 and the procurement is complete. The [redacted] is on schedule to be deployed and operational by the June 30, 2018 estimated completion date.

Any questions regarding this response should be directed to Rack Campbell at (703) 516-1422) or Kim Farrell at (703) 516-5101.

cc: Marshall E. Gentry, Deputy Director, DOF, Risk Management and Internal Control
Russell G. Pittman, Director, DIT
Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Rack D. Campbell, Chief, DIT, Audit and Internal Control Section

5

FDIC

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

DATE: July 25, 2018

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

FROM: Howard G. Whyte [redacted]
Chief Information Officer and Chief Privacy Officer

Zachary N. Brown [redacted]
Chief Information Security Officer

SUBJECT: Advisory Memorandum Entitled *Administration of Network Firewalls* (Assignment No. 2017-012) - Progress Update

Thank you for the opportunity to provide a progress update on the status of the corrective actions included in the management's response to the Office of Inspector General's (OIG) Advisory Memorandum on the *Administration of Network Firewalls*, issued February 9, 2018. In its memorandum, the OIG documented three primary concerns regarding the administration of the FDIC's network firewalls.

Our response provides a description of the progress the Chief Information Officer (CIO) Organization has made to address the risks described in the OIG's memorandum including the timeframes for completing those actions. Our response is organized by the areas of concern raised by the OIG and contains actions planned or in process and the current status as of July 17, 2018.

We appreciate your staff's time and effort and we expect that the actions taken in response to this advisory memorandum will further enhance the FDIC's network firewall controls and reduce risk to the agency. Cybersecurity is essential in protecting the FDIC's data and systems and it remains a top priority.

MANAGEMENT RESPONSE

Advisory Area 1 – Lack of Documentation for Firewall Rules

The FDIC's network [redacted] (as of September 7, 2017). FDIC has not properly documented a number of its firewall rules with supporting explanations of the associated business need, nor has the FDIC documented approvals for these firewall rules. In November 2017, OIG reviewed a sample of nine outbound rules in the [redacted] firewalls and requested business justifications. On December 4, 2017, an FDIC firewall administrator advised he determined that eight of these rules did not serve a current business need and, therefore, he disabled the eight rules. Two days later, the Acting Chief Information Security Officer (CISO) advised that the rules we inquired about were implemented before the CIO Organization established a formal process for firewall rules. As a result, the CIO Organization did not have any documentation as to who requested the rules, what business needs supported the rules, or who approved the rules for implementation. On January 26, 2018, the Acting CISO advised that the FDIC had identified a large number of rules that did not have a documented business justification and/or had not been used recently. The lack of proper documentation limits the FDIC's ability to review firewall rules effectively to determine whether they continue to serve a business need.

Management Decision: Concur

Corrective Action:
[redacted]. The OCISO has begun a remediation effort to remove the unused rules and ensure undocumented rules are updated to match the current standard (defined in the Firewall Change Request Process v2.0 document). The scope of this review includes both the [redacted] firewalls. Status reports are provided to OCISO management on a weekly basis.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
The process of requiring business justification on new rules has been in place since 2013.
[redacted]

Estimated Completion Date: March 31, 2018

Status as of April 19, 2018:
The manual review of both the [redacted] firewall rules was completed on schedule. OCISO removed unused rules and validated the remaining rules were consistent with the current configuration standard, as defined in the Firewall Change Request Process v2.0. The final status report was provided to the Acting CISO on April 2, 2018.

2

Status as of July 17, 2018:
OCISO is performing a secondary review to ensure all rules are accurately documented. This secondary review is scheduled for completion on August 17, 2018.

Advisory Area 2 – Manual Review of Firewall Rules

FDIC firewall administrators advised that they manually review firewall rules. However, these reviews are not documented. Manually reviewing thousands of rules is cumbersome and impractical, and places a considerable burden on firewall administrators to ensure that the rules are still needed and properly configured. A firewall administrator advised that the firewall team only has time to manually review a relatively small portion of the network firewall ruleset each quarter. The manual reviews were complicated by the lack of documentation for many firewall rules. Without documentation, firewall administrators must, in many instances, research who requested the rule and the basis for the request. Weaknesses in the firewall review process allowed unnecessary firewall rules to go undetected, thus increasing the risk that the [redacted]

Management Decision: Concur

Corrective Action:
[redacted]. Standard Operating Procedures will be created to address all process changes. Additionally, the OCISO has obtained business analyst support to assist in identifying any operational tasks that lack supporting documentation. The status of this effort is reported to CIOO executive management in the CIOO weekly management report.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
[redacted]

3

Estimated Completion Date:

- Complete business analysis assessment: February 28, 2018
- Remove unused/redundant/shadow rules: March 31, 2018
- Ensure rules have associated [redacted] change numbers: March 31, 2018
- [redacted]
- [redacted]
- Update/Create Standard Operating Procedures: On-going

Status as of April 19, 2018:
The business analyst assessment performed to identify any operational tasks that lack supporting documentation was completed on schedule and delivered to the Acting CISO on February 16, 2018. The assessment identified eight out of fourteen SOPs requiring revision and four new SOPs that should be drafted to document recurring work. Work to update and create Firewall Support SOPs is ongoing.

The manual review of firewall rules to identify rulesets that were redundant, inconsistent with the current configuration standard, or no longer used was completed on schedule. The [redacted] being implemented to automate the reporting of unused policies was reviewed and approved at the April 12, 2018 meeting of the Security and Enterprise Architecture Technical Advisory Board (SEATAB), and the procurement is complete.

Status as of July 17, 2018:
OCISO is performing a secondary review to ensure all rules are accurately documented. This secondary review is scheduled for completion on August 17, 2018.

Furthermore, OCISO is working with [redacted] for assistance with integration into the environment. The vendor will setup the automated functionality of the [redacted] (i.e. reporting, alerting, and ticketing).

Advisory Area 3 – Lack of an Automated Tool to Review Firewall Rules.

There are a number of automated tools available to facilitate the review of firewall rulesets. Such tools can be used to identify rules that are redundant or inconsistent with security policies; flag rules that are no longer used, and help document justifications for rules. On January 26, 2018, the Acting CISO advised that the FDIC firewall administrators had implemented an automated firewall tool [redacted] earlier in the month to analyze the firewall ruleset. The CIO Organization originally purchased the [redacted] tool in July 2011; however, the tool remained in a test environment until January 2018. As a result, the FDIC has received little value for the licensing fees it has paid for the [redacted] tool since 2011. Further, firewall administrators have determined that the functionality of the [redacted] tool does not meet their needs. Therefore, FDIC firewall administrators are evaluating other tools for the FDIC environment.

Management Decision: Concur

4

Corrective Action:
The OCISO has evaluated and selected the [redacted] to support this requirement. [redacted] The OCISO is in the process of procuring the product.

The [redacted] will be used to automate significant pieces of the firewall rule review process. Specifically, it will automate reporting of unused and redundant rules, and alerting when rules are added [redacted] will also be integrated with [redacted] to streamline and gain efficiencies in workflow processing of the rule reviews.

Existing or Planned Compensating Controls that Mitigate or Reduce Risk:
The OCISO is leveraging the results identified during the evaluation period. The [redacted] is in procurement, and is scheduled to be deployed in production in Q2 2018.

Estimated Completion Date: June 30, 2018

Status as of April 19, 2018:
The [redacted] was reviewed and approved during the SEATAB meeting held on the April 12, 2018 and the procurement is complete. The [redacted] is on schedule to be deployed and operational by the June 30, 2018 estimated completion date.

Status as of July 17, 2018:

As stated above, OCISO is working with [redacted] for assistance with integration into the environment. The vendor will setup the automated functionality of the [redacted] (i.e. reporting, alerting, and ticketing).

Any questions regarding this response should be directed to Rack Campbell at (703) 516-1422 or Steve Matthews at (703) 516-5050.

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Control
Russell G. Pittman, Director, DIT
Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Rack D. Campbell, Chief, DIT, Audit and Internal Control Section

5

FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990 Chief Information Officer Organization

DATE:	April 15, 2019
TO:	Mark F. Mulholland Assistant Inspector General for Information Technology Audits and Cyber Office of the Inspector General
THROUGH:	Howard G. Whyte **/Signed/** Chief Information Officer and Chief Privacy Officer Chief Information Officer Organization
FROM:	Zachary N. Brown **/Signed/** Chief Information Security Officer Office of the Chief Information Security Officer Russell G. Pittman **/Signed/** Director Division of Information Technology
SUBJECT:	Management Response to the Draft Audit Report Entitled *Preventing and Detecting Cyber Threats* (Assignment No. 2017-012)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on *Preventing and Detecting Cyber Threats* issued on March 27, 2019. The Federal Deposit Insurance Corporation's (FDIC) cyber threat detection and prevention activities are critical to the agency's ability to carry out the mission of maintaining stability and public confidence in the nation's financial system. Cybersecurity, including the prevention and detection of cyber threats, is a top management priority at the FDIC.

The purpose of the audit was to assess the effectiveness of two security controls intended to prevent and detect cyber threats on the FDIC's network: (i) Firewalls; and (ii) the Security Information and Event Management (SIEM) tool. The FDIC does not rely solely on the SIEM tool and firewalls to prevent and detect cyber attacks. The FDIC implements multiple layers of security mechanisms to prevent and detect cyber threats in its information technology environment.

During the course of the audit, which began in October 2017, the Chief Information Officer Organization (CIOO) made significant progress in maturing the management and administration of firewall and SIEM related security controls. The CIOO has conducted several reviews of existing firewall rules and established policy and process for continued improvements in maintaining firewall rules and documentation to support the mission/business need and duration of that need. Among these improvements, the CIOO established a Firewall and Network Security Policy, revised the change request and review process, updated the Secure Baseline Configuration Guides for network security devices, and formalized a framework for managing the lifecycle of use cases in the SIEM tool.

Page 1 of 7

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Chief Information Officer Organization

In its report, the OIG audit team made ten (10) recommendations to the CIOO. We have carefully considered and concur with each of the recommendations. The CIOO completed actions for five (5) of the ten (10) recommendations. This response outlines the CIOO's completed or planned corrective actions and the corresponding completion dates.

As noted in the report, the FDIC took steps to improve restrictions on access to network firewalls and ensured production perimeter firewalls are being monitored for baseline configuration deviations. The issues that are identified in the report represent opportunities for the FDIC to better ensure that controls are enchanced and formally documented. We look forward to continuing a productive dialogue with the OIG in the coming months on the FDIC's efforts to address the areas noted in the report.

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Chief Information Office Organization

MANAGEMENT RESPONSE

Recommendation 1

We recommend that the CIO:

1. Require that all existing firewall rules be documented with an approval and mission/business need, including the duration of that need.

Management Decision: Concur

Corrective Action:

The CIOO established a process requiring existing firewall rules be documented with an approval, business justification, and duration of that need on March 18, 2019. The CIOO conducted a complete review of all existing firewall rules to determine compliance with CIOO policy and updated firewall procedures. As a result of the review, the CIOO identified additional remediation efforts that will continue through January 31, 2020.

Estimated Completion Date: January 31, 2020

Recommendation 2

We recommend that the CIO:

2. Establish and implement firewall policy consistent with NIST guidance.

Management Decision: **Concur**

Corrective Action:

On March 8, 2019, CIOO issued Policy 19-002, "Policy on Firewall and Network Security," which established security requirements for FDIC firewalls and network infrastructure. The CIOO will fully implement this policy by January 31, 2020.

Estimated Completion Date: January 31, 2020

Recommendation 3

We recommend that the CIO:

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Chief Information Officer Organization

3. Establish and implement a procedure to conduct reviews of firewall rules by individuals who are not part of the firewall administration process.

Management Decision: Concur

Corrective Action:

CIOO issued Policy 19-002, "Policy on Firewall and Network Security," which requires CIOO to conduct an annual review of firewall rules to provide reasonable assurance that the appropriate security controls are operating as intended. CIOO created a Standard Operating Procedure for conducting the annual independent firewall review. The CIOO will provide evidence to demonstrate completion of an independent review in accordance with the documented procedure by May 3, 2019.

Estimated Completion Date: May 3, 2019

Recommendation 4

We recommend that the CIO:

4. Require that the quarterly reviews of firewall rules by administrators be documented.

Management Decision: Concur

Corrective Action:

The CIOO updated its Firewall Rule Review Standard Operating Procedure to require the quarterly firewall reviews be conducted and documented by the firewall administrators. The updated procedure was completed on April 12, 2019. CIOO has completed the quarterly review and will provide evidence to demonstrate completion of the review by April 26, 2019.

Estimated Completion Date: April 26, 2019

Recommendation 5

We recommend that the CIO:

5. Establish and implement a requirement to review the National Checklist Repository on a regular basis; update the FDIC's baseline configurations for network firewalls; and document the results of the review.

Management Decision: Concur

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Chief Information Officer Organization

Corrective Action:

CIOO revised the Secure Baseline Configuration Process to require the quarterly review of firewall configurations against the National Checklist Repository to ensure they remain current. Additionally, CIOO updated the Secure Baseline Configuration Guides for network security devices to reflect the most current security configuration settings recommended by NIST. CIOO performed compliance scans against the updated baselines and created Plan of Action & Milestones (POA&M) to track the remediation of deviations identified. CIOO will provide evidence to demonstrate implementation of this new requirement by May 24, 2019.

Estimated Completion Date: May 24, 2019

Recommendation 6

We recommend that the CIO:

6. Review all [redacted] firewalls and remove any local accounts that are not permitted by the approved baseline configuration.

Management Decision: Concur

Corrective Action:

The CIOO completed a review of all [redacted] firewalls and removed local accounts that are not permitted per the approved secure baseline configuration on March 20, 2019.

Estimated Completion Date: Completed-March 20, 2019.

Recommendation 7

We recommend that the CIO:

7. Perform a documented analysis to determine [redacted].

Management Decision: Concur

Corrective Action:

The CIOO completed a documented analysis to determine [redacted]

Estimated Completion Date: Completed-March 27, 2019.

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Chief Information Officer Organization

Recommendation 8

We recommend that the CIO:

8. Clarify policies and procedures to define [redacted] accounts that are required to be managed [redacted]

Management Decision: Concur

Corrective Action:

[redacted]

The FDIC also updated relevant procedures to assist in ensuring compliance with this requirement. The memorandum and revised procedure were published on April 12, 2019.

Estimated Completion Date: Completed-April 12, 2019.

Recommendations 9

We recommend that the CIO:

9. Document, approve, and implement a structured process for identifying, developing, prioritizing, deploying, maintaining, and retiring Use Cases for the SIEM tool.

Management Decision: Concur

Corrective Action:

The CIOO formalized the process for identifying, developing, prioritizing, deploying, maintaining, and retiring Use Cases for the SIEM tool on March 26, 2019. The CIOO will continuously improve the Use Cases process for the SIEM tool to enhance security monitoring.

Estimated Completion Date: Completed-March 26, 2019.

Recommendations 10

10. Document, approve, and implement a process to test and update Use Cases periodically in order to ensure they operate as intended.

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Chief Information Officer Organization

Management Decision: Concur

Corrective Action:

The CIOO formalized the process for maintaining Use Cases for the SIEM tool which includes periodic testing and updating of Use Cases on March 26, 2019. The CIOO will continuously improve the Use Cases process for the SIEM tool to enhance security monitoring.

Estimated Completion Date: Completed-March 26, 2019.

If you have any questions regarding this response, please contact Jennah Mathieson, Acting Chief, Information Technology Rick, Governance, and Policy Section and Director, Office of CIO Management Services, DIT on 703-516-5228.

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

Summary of the FDIC's Corrective Actions

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 CIOO established a process on March 18, 2019 requiring that existing firewall rules be documented with an approval, business justification, and duration of that need. In addition, the CIOO reviewed existing firewall rules to determine compliance with CIOO policy and updated its firewall procedures. As a result of the review, the CIOO identified the need for additional remediation efforts.	January 31, 2020	$0	Yes	Open
2	The CIOO issued Policy 19-002, *Policy on Firewall and Network Security*, on March 8, 2019. The policy established security requirements for the firewalls and network infrastructure. The CIOO will fully implement this policy.	January 31, 2020	$0	Yes	Open
3	The CIOO issued Policy 19-002, *Policy on Firewall and Network Security*, which requires the CIOO to conduct an annual review of firewall rules. The CIOO also created a Standard Operating Procedure for conducting the annual firewall review. The CIOO will provide evidence that the annual firewall review has been completed in accordance with the Standard Operating Procedure.	May 3, 2019	$0	Yes	Open
4	The CIOO updated its Firewall Rule Review Standard Operating Procedure on April 12, 2019 to require firewall administrators to conduct and document quarterly firewall reviews. The CIOO completed the quarterly review and will provide evidence of its completion.	April 26, 2019	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
5	The CIOO revised the Secure Baseline Configuration Process to require a quarterly review of firewall configurations against the National Checklist Repository. The CIOO also updated the Secure Baseline Configuration Guides for network security devices to reflect current security configuration settings recommended by NIST. Further, the CIOO performed compliance scans against the updated baselines and created Plans of Action & Milestones (POA&M) to track remediation of identified deviations. The CIOO will provide evidence that it has implemented this new requirement.	May 24, 2019	$0	Yes	Open
6	The CIOO reviewed all [redacted] firewalls and removed local accounts that were not permitted by the approved baseline configuration.	March 20, 2019	$0	Yes	Closed
7	The CIOO documented an analysis to determine [redacted].	March 27, 2019	$0	Yes	Closed
8	[redacted]. The CIOO also updated relevant procedures to help ensure compliance with this requirement.	April 12, 2019	$0	Yes	Closed
9	The CIOO formalized the process for identifying, developing, prioritizing, deploying, maintaining, and retiring Use Cases for the SIEM tool on March 26, 2019. The CIOO will continuously improve the Use Case process for the SIEM tool.	March 26, 2019	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
10	The CIOO formalized a process for maintaining Use Cases for the SIEM tool on March 26, 2019. The process includes periodic testing and updating of Use Cases. The CIOO will continuously improve the Use Cases process for the SIEM tool.	March 26, 2019	$0	Yes	Closed

[a] Recommendations are resolved when —

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

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

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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

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