Sharing of Threat Information to Guide the Supervision of Financial Institutions

January 2022 **AUD-22-003**

Audit Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

REDACTED VERSION

PUBLICLY AVAILABLE

The redactions contained in this report are based upon requests from FDIC senior management to protect the Agency's information from disclosure.

Office of Inspector General

Executive Summary

Sharing of Threat Information to Guide the Supervision of Financial Institutions

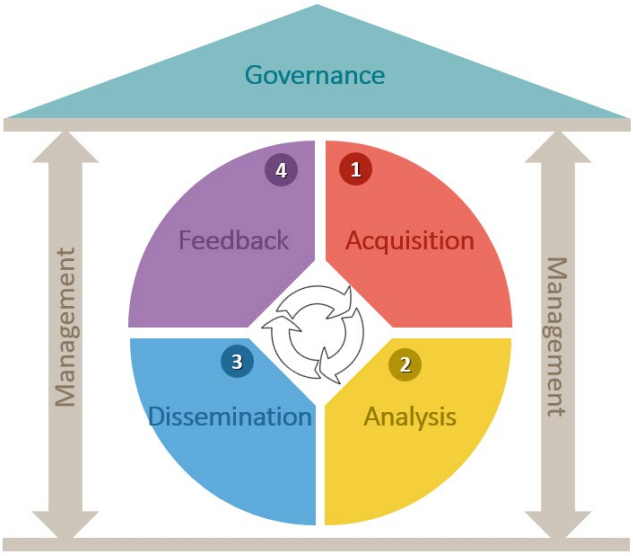
Financial institutions face a wide range of threats to their operations, including cyber attacks, money laundering, terrorist financing, pandemics, and natural disasters. Further, the interconnected nature of financial services increases the potential impact that threats can have on financial institutions. For example, many financial institutions rely on third-party service providers that deliver critical banking services. An incident at a third-party provider that services many financial institutions could have a cascading impact on financial services. Such incidents have the potential to disrupt the delivery of vital financial services, inflict financial harm on consumers, and jeopardize the safety and soundness of financial institutions. If the impact becomes widespread, it could diminish public confidence, impact the Deposit Insurance Fund, and destabilize the United States financial system.

To fulfill its mission, the FDIC acquires, analyzes, and disseminates threat information relating to cyber and other threats to the financial sector and FDIC operations. Effective sharing of threat information helps to build situational awareness, support risk-informed decision-making, and influence supervisory strategies, policies, and training. Several component offices within the FDIC play critical roles in threat information sharing.

The Operational Risk group within the Division of Risk Management Supervision (RMS) works to identify, monitor, analyze, and share information about operational risks that can threaten the safety and soundness of FDIC-supervised financial institutions. In addition, the FDIC's intelligence support program and its related functions (hereinafter, "Intelligence Support Program") within the Division of Administration (DOA) provides FDIC executive management and staff with threat information that can affect the FDIC, its insured financial institutions, and the Financial Services Sector.

The FDIC's threat information sharing activities can be organized into four life cycle components: (1) acquiring relevant and actionable threat information from internal and external sources; (2) analyzing threat information to determine how it can support programs, operations, and decision-making; (3) disseminating threat information to stakeholders who need it; and (4) obtaining feedback from stakeholders regarding how the use of threat information can be improved.

Figure: The Threat Sharing Framework



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

The Government Accountability Office (GAO), the Office of Management and Budget, and private sector organizations have published standards, guidance, and practices associated with successful program and project management. These standards, guidance, and practices include elements of effective Governance, such as written policies and procedures, defined roles and responsibilities, and goals and objectives. They also include elements of effective Management, such as succession and contingency planning for key staff, employee training, and information security risk management. The Figure illustrates the four life cycle components of threat information sharing and their relationship to Governance and Management controls.

The audit objective was to determine whether the FDIC established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The audit focused on the FDIC's internal processes for sharing threat information with personnel in its Headquarters, Regional, and Field Offices.

Results

We found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The FDIC acquired and analyzed certain information pertaining to threats against FDIC-supervised financial institutions and disseminated this information to supervisory personnel in its Headquarters, Regional,

and Field Offices. However, we identified gaps in each component of the Threat Sharing Framework. Specifically, the FDIC did not:

- Establish a written governance structure to guide its threat information sharing activities;
- Complete, approve, and implement a governance Charter that established a common understanding of the role for the Intelligence Support Program or defined an overall strategy and requirements for it;
- Develop goals, objectives, or measures to guide the performance of its Intelligence Support Program;
- Establish adequate policies and procedures that defined roles and responsibilities for key stakeholders involved in the threat information sharing program and activities; and
- Fully consider the risks discussed in this report for its Enterprise Risk Inventory and Risk Profile.

We also identified gaps in the FDIC's processes for acquiring, analyzing, and disseminating threat information, and in its processes for obtaining feedback from stakeholders regarding how the use of threat information can be improved.

- **Acquisition.** The FDIC did not develop written procedures for determining its threat information requirements. In addition, the FDIC did not engage all relevant stakeholders when it developed its *Information Needs Document*, which contains the FDIC's threat information requirements. As a result, the FDIC has limited assurance that it will acquire all relevant threat information to support its business operations and programs.

  In addition, existing Federal regulations do not require prompt reporting of certain destructive cyber incidents that could threaten the safety and soundness of insured financial institutions. Such reporting would provide the FDIC and other Federal bank regulators vital information needed to effectively assess threats and implement timely supervisory actions.

- **Analysis.** The FDIC did not establish procedures to guide its analysis of threat information. Absent such procedures, the FDIC relied solely on the discretionary judgment of certain individuals to determine the extent to which threat information should be analyzed to support FDIC business needs and the supervision of financial institutions. Without procedures, there is limited

assurance that the threat analysis it performs is consistent and sufficient to address the needs of its stakeholders. Procedures would also help to ensure a smooth transition of knowledge to new analysts when staff depart the FDIC. Further, expanding the scope and depth of threat analysis could provide the FDIC with more effective threat information.

- **Dissemination.** The FDIC did not develop procedures for disseminating threat information. Absent such procedures, decisions regarding what to disseminate, to whom, and when, are left solely to the discretion of individuals, which could lead to inconsistent or untimely communications.

  In addition, the FDIC required its Regional Directors to hold high-level security clearances, so these personnel could access classified information in the performance their duties. However, we found that the Regional Directors rarely or never received classified information and the FDIC had not established an infrastructure that would allow for the secure handling of such information to the Regional Offices. Such infrastructure includes the systems and protocols for the secure dissemination, communication, use, storage, and disposition of classified information.

- **Feedback.** The FDIC did not establish a procedure to obtain feedback from recipients of threat information to assess its utility and effectiveness. Such structured feedback could provide valuable information regarding the extent to which FDIC personnel use threat information to build situational awareness and influence supervisory decision-making.

We also identified gaps in the FDIC's management control activities. Specifically, the FDIC did not establish an alternate (backup) for its Senior Intelligence Officer (SIO) position, or develop a succession plan to mitigate the risk of a prolonged absence or departure of the SIO. Since April 12, 2021, the SIO has been serving on a detail assignment, and the FDIC has not named a replacement to fill the SIO position.

In addition, the FDIC did not establish minimum training requirements for the SIO position to ensure the continued development and retention of knowledge, skills, and abilities. Further, the FDIC did not obtain required security clearances for two of its six Regional Directors, as specified in the Regional Director position description, until we identified the exceptions during this audit. Finally, the FDIC did not categorize unclassified threat information managed by the SIO consistent with security standards and guidance issued by the National Institute of Standards and Technology (NIST).

Recommendations

The report contains 25 recommendations. The report recommends that the FDIC establish and implement a Charter, goals, objectives, and measures to govern the Intelligence Support Program. The report also recommends that the FDIC establish and implement policies and procedures that define roles and responsibilities for acquiring, analyzing, and disseminating threat information managed by the Intelligence Support Program and the RMS Operational Risk group. In addition, the report recommends that the FDIC Enterprise Risk Inventory and Risk Profile fully consider the threat information sharing risks identified in this report.

The report recommends that the FDIC update and approve its *Information Needs Document* to ensure it includes all relevant threat information requirements. Further, the report recommends that the FDIC evaluate whether the scope and depth of threat analysis needs to be expanded to more effectively assess threats to financial institutions, and require supervised financial institutions to promptly report destructive cyber incidents. The report recommends that the FDIC establish a means to disseminate classified information to its Regional Offices in a timely manner so that the information is actionable; determine whether additional Regional Office personnel should hold security clearances; and implement a procedure to assess the effectiveness of its threat sharing activities.

The report recommends that the FDIC establish a backup and succession plan for the SIO; require unclassified threat information managed under the Intelligence Support Program to be stored on a centralized platform; and establish minimum training requirements for the SIO.

Moreover, the report recommends that the FDIC implement control improvements to ensure that requests for security clearances are processed in a timely manner, and threat information is inventoried, categorized, and secured consistent with NIST security standards and guidelines.

The FDIC concurred with 22 recommendations, partially concurred with 2 recommendations, and non-concurred with one recommendation of the 25 recommendations in this report. The FDIC plans to complete all corrective actions by December 16, 2022.

Office of Inspector General

Contents

Appendices

Figures

January 18, 2022

Subject ***Sharing of Threat Information to Guide the Supervision of Financial Institutions***

The Federal Deposit Insurance Corporation (FDIC) plays a critical role in maintaining stability and public confidence in our Nation's financial system. As of March 31, 2021, the FDIC insured approximately $16.9 trillion in deposits at 4,978 commercial banks and savings institutions.[1] The FDIC also served as the primary Federal regulator for 3,209 of these institutions, and the backup regulator for the remaining 1,769 institutions. In addition, the FDIC has statutory authority to manage the resolution of some of the largest and most complex financial institutions in the world.[2]

These financial institutions face a wide range of threats[3] to their operations. Such threats include cyber attacks, money laundering, terrorist financing, pandemics, and natural disasters. Further, the interconnected nature of financial services increases the potential impact that threats can have on financial institutions. For example, many financial institutions rely on third-party service providers that deliver critical banking services. An incident at a third-party provider that services many financial institutions could have a cascading impact on financial services. Such incidents have the potential to disrupt the delivery of vital financial services, inflict financial harm on consumers, and jeopardize the safety and soundness of financial institutions. If the impact becomes widespread, it could diminish public confidence, impact the Deposit Insurance Fund, and destabilize the United States financial system.

[1] FDIC *Quarterly Banking Profile* (First Quarter 2021).
[2] Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, as amended, (the Dodd-Frank Act), the FDIC has the authority to manage the orderly failure of large, complex, systemically important financial institutions. This authority applies when an institution's failure through bankruptcy would cause severe adverse consequences to the U.S. financial system or economy. 12 U.S.C. Section 5301.
[3] The Department of Homeland Security (DHS) defines the term, "threat," as "a natural or human-created occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property." See *DHS Risk Lexicon Terms and Definitions*, 2017 Edition – Revision 2 (October 2017, DHS Risk Lexicon).

As part of its mission, the FDIC acquires, analyzes, and disseminates threat information[4] to inform senior FDIC officials and decision-makers, its supervisory program, and insured financial institutions. Effective sharing of threat information builds situational awareness, supports risk-informed decision-making, and influences supervisory strategies, policies, and training. To ensure that these efforts are efficient and effective, the FDIC should have appropriate processes in place to guide its threat information sharing activities.

Our audit objective was to determine whether the FDIC established effective processes to acquire[5], analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The audit focused on the FDIC's internal processes for sharing threat information with personnel in its Headquarters, Regional, and Field Offices. The audit also considered how the FDIC's threat information sharing processes support other business needs, such as resolution planning, information security risk management, and emergency preparedness.

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 list of acronyms and abbreviations; Appendix 3 contains both an Advisory Memorandum issued by the Office of Inspector General (OIG) to FDIC management regarding the need for financial institutions to promptly report destructive[6] cybersecurity incidents, accompanied by FDIC management's response; Appendix 4 contains both an Advisory Memorandum issued by the OIG to FDIC management describing the potential exposure of certain insured financial institutions to the SolarWinds, Inc. (SolarWinds) compromise and FDIC management's response; and Appendix 5 and

[4] According to NIST, threat information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, and threat intelligence. For this report, we use the term "threat information" to include threat intelligence. According to NIST, threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

[5] By acquire, we mean obtain and not purchase.

[6] We use the term, "destructive," because the Federal Financial Institutions Examination Council (FFIEC) uses this term in its Joint Statements, such as the *Joint Statement, Destructive Malware* (March 2015), and in its *Business Continuity Management* booklet, which is a component of the *FFIEC Information Technology Examination Handbook*. The FFIEC is an interagency body empowered to (1) prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the FDIC, the Board of Governors of the Federal Reserve System (Federal Reserve Board), the National Credit Union Association (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and (2) make recommendations to promote uniformity in the supervision of financial institutions.

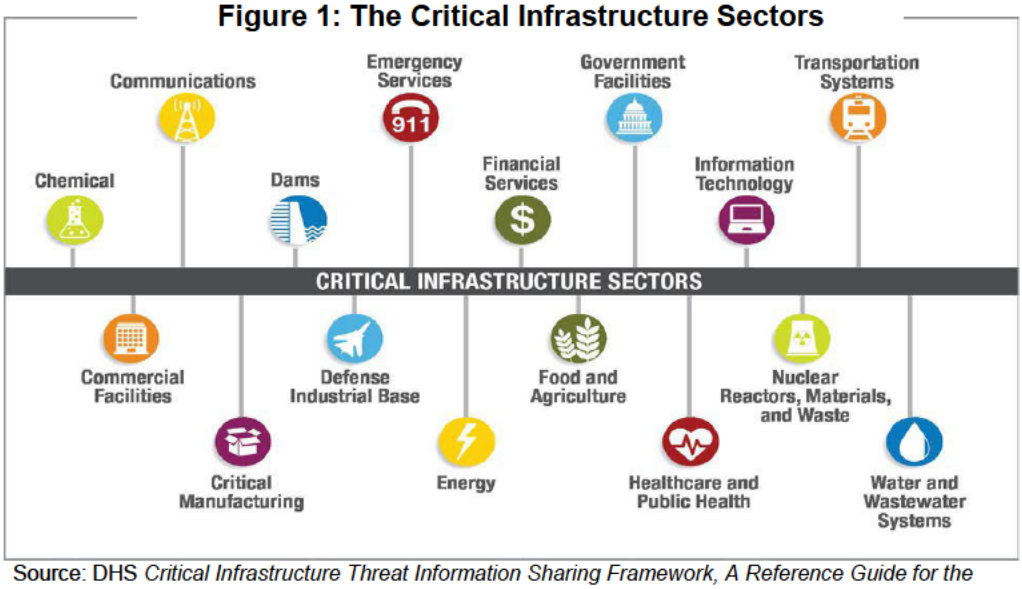
Appendix 6 contain the FDIC's comments on this report and a summary of the FDIC's corrective actions.

BACKGROUND

Presidential Policy Directive 21 (PPD 21), *Critical Infrastructure Security and Resilience* (February 2013), established a national policy for strengthening the security and resilience of the Nation's critical infrastructure. The term, "critical infrastructure," refers to "systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these."[7] According to PPD 21, protecting the Nation's critical infrastructure is a shared responsibility among Federal, state, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure (hereinafter Critical Infrastructure Stakeholders).

PPD 21 divides the Nation's critical infrastructure into 16 sectors (see Figure 1). PPD 21 also designates a Federal department or agency, known as a Sector-Specific Agency, to lead a collaborative process for critical infrastructure security within each of the 16 sectors. The U.S. Department of the Treasury (Treasury Department) serves as the Sector-Specific Agency for the Financial Services Sector. In this role, the Treasury Department coordinates with the FDIC and other Critical Infrastructure Stakeholders to protect the Nation's financial services.

Figure 1: The Critical Infrastructure Sectors



Source: DHS *Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community* (October 2016)

[7] USA PATRIOT Act, 42 U.S.C. §5195c (e).

Sector-Specific Agencies are responsible for developing and implementing Sector-Specific Plans that establish goals and priorities for addressing threats based on the unique operating conditions and risk landscape of each sector. Accordingly, the Treasury Department coordinated with other public and private sector entities in the Financial Services Sector to develop the *Financial Services Sector-Specific Plan 2015*. This plan provides an overview of the Financial Services Sector and the cybersecurity and physical risks it faces; establishes a strategic framework that serves as a guide for prioritizing the sector's day-to-day work; and describes key mechanisms for implementing and assessing the strategic framework. The *Financial Services Sector-Specific Plan 2015* enables the integration of security and resilience efforts in the Financial Services Sector with a broader National framework of critical infrastructure activities.[8]

The FDIC's Role in the Financial Services Sector

The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and equities and derivatives markets. The FDIC plays a critical role in maintaining stability and public confidence in the Financial Services Sector. The FDIC protects millions of depositors of insured banks in the United States against the loss of their deposits if their bank fails. In addition to insuring deposits, the FDIC acts as receiver when an insured financial institution fails. As receiver, the FDIC sells the institution's assets and settles its debts.

According to the *Financial Services Sector-Specific Plan 2015*, FDIC-insured financial institutions are the primary providers of wholesale and retail payment services in the Financial Services Sector. These payment services include wire transfer systems, checking accounts, and credit and debit cards. FDIC-insured financial institutions also provide customers with various forms of credit, such as mortgages and home equity loans, collateralized and uncollateralized loans, and lines of credit including credit cards.

The FDIC's Supervision Program

The FDIC implements a supervision program to promote safe and sound operations at insured financial institutions. Pursuant to its authorities under the Federal Deposit

[8] The *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* defines the broader national framework for managing risks to the Nation's critical infrastructure. This plan outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

Insurance (FDI) Act (12 U.S.C. Section 1811), the FDIC serves as the primary Federal regulator for state-chartered financial institutions that are not members of the Federal Reserve System.[9] Within the FDIC, the Division of Risk Management Supervision (RMS) has primary responsibility for implementing the supervision program. The supervision program is intended to help ensure that FDIC-supervised financial institutions operate in a safe and sound manner and comply with banking laws and regulations in the provision of financial services.

RMS conducts risk management examinations of FDIC-supervised financial institutions to assess their overall financial condition, management practices and policies, and compliance with applicable laws and regulations. RMS also conducts specialty examinations covering information technology (IT) and operations, Bank Secrecy Act (BSA) and anti-money laundering compliance, and trust department operations.

The Large Bank Supervision Branch of RMS coordinates with the Regional and Area Offices to supervise Large Insured Depository Institutions (LIDIs). LIDIs are institutions with total assets of at least $10 billion. As of June 30, 2021, the FDIC oversaw 112 LIDIs with total combined assets of $4.18 trillion.

The FDIC, the Federal Reserve Board, and state banking agencies coordinate to examine and monitor insured state-chartered financial institutions. These bank regulatory agencies coordinate on policy, training, and other matters through various forums, such as the FFIEC and the Conference of State Bank Supervisors (CSBS). Further, the FDIC coordinates with the Federal Reserve Board and the Office of the Comptroller of the Currency (OCC) to conduct examinations of significant service providers that contract with insured financial institutions.[10]

[9] The FDIC, the Federal Reserve Board, the OCC, and the NCUA have primary responsibility for regulating insured financial institutions at the Federal level. The Federal Reserve Board regulates state-chartered institutions that are members of the Federal Reserve System; the OCC regulates Federally-chartered institutions; and the NCUA regulates Federally- and state-chartered credit unions.
[10] The Bank Service Company Act authorizes the FDIC, the Federal Reserve Board, and the OCC to examine contractual services provided by third parties to insured financial institutions. 12 U.S.C. Section 1867(c) (1).

Large and Complex Financial Institutions

The Dodd-Frank Act provided the FDIC with the authority to resolve financial companies for which the bankruptcy process is not viable.[11] The FDIC's Division of Complex Institution Supervision and Resolution (CISR) fulfills this statutory authority by implementing monitoring and resolution programs for large and complex financial institutions (LCFIs). In July 2019, the FDIC created CISR to centralize and integrate the FDIC's operations related to the monitoring and resolution of LCFIs.

LCFIs include global systemically important banks (GSIBs) and all insured depository institutions with assets above $100 billion for which the FDIC does not serve as the primary Federal regulator. LCFIs also include other systemically important financial institutions (SIFIs) whose failure could potentially threaten U.S. financial stability and trigger implementation of the Orderly Liquidation Authority under the Dodd-Frank Act. As of June 2021, the FDIC provided oversight of 37 LCFIs.

Threats Against Financial Institutions

Financial institutions face an evolving and dynamic set of operational threats.

Cyber Attacks. In January 2020, the FDIC and the OCC issued a *Joint Statement on Heightened Cybersecurity Risk* which stated that disruptive and destructive cyber attacks against financial institutions have increased in frequency and severity in recent years. According to this Joint Statement, threat actors often use destructive malware to exploit weaknesses in information systems at financial institutions. The Joint Statement further states that destructive malware has the potential to alter, delete, or otherwise render a financial institution's data and systems unusable, as well as backup systems.

One type of destructive malware that threat actors have used to victimize financial institutions is Ransomware. The Department of Justice has described Ransomware as a "growing threat" with the potential to inflict "destructive and devastating consequences" on the Nation's critical infrastructure.[12] Ransomware actors often pressure their victims to pay ransoms by threatening to release stolen data if the

[11] The Dodd-Frank Act requires failed or failing financial companies to file for reorganization or liquidation under the U.S. Bankruptcy Code. However, if the company's resolution under the Bankruptcy Code would result in serious adverse effects to U.S. financial stability, Title II of the Dodd-Frank Act provides an Orderly Liquidation Authority that can be invoked. The Orderly Liquidation Authority can only be invoked under a statutorily prescribed recommendation and determination process, coupled with an expedited judicial review process.

[12] Memorandum from the Deputy Attorney General to all Federal prosecutors, entitled *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021).

victims refuse to pay.[13] Victims may pay a ransom in exchange for a decryption key that unlocks their systems and data. Ransomware can severely disrupt a financial institution's operations by encrypting its systems and data, until the institution pays a ransom. In March 2020, a large service provider experienced a Ransomware attack that disrupted the operations of financial institutions around the globe, including 21 FDIC-insured institutions.

Financial institutions also face a wide range of other cyber threats, such as denial-of-service attacks,[14] and theft of sensitive information. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC)[15] reported that a threat actor targeted more than 100 financial services firms around the world in 2020 in a wave of distributed denial-of service extortion attacks. In addition, in 2014, JPMorgan Chase and Company disclosed that it had experienced a breach[16] that compromised information related to 76 million households and 7 million small businesses.[17]

Money Laundering. In December 2018, the Treasury Department issued its *National Money Laundering Risk Assessment*, which identified money laundering as a significant concern because it facilitates and conceals crime and can distort markets and the broader financial system. Financial institutions are responsible for developing and administering a program to assure and monitor compliance with the BSA—a statute intended to facilitate the detection and prevention of money laundering.[18] The Federal bank regulators, including the FDIC, regulate and examine financial institutions under their supervision for compliance with the BSA. Financial institutions that do not implement adequate BSA/AML programs can face significant fines and other enforcement actions.

[13] See DHS's Cybersecurity and Infrastructure Security Agency's (CISA) statement, entitled *CISA Launches Campaign To Reduce The Risk Of Ransomware* (January 2021; updated February 2021).
[14] According to CISA, a denial-of-service attack occurs when legitimate users cannot access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.
[15] FS-ISAC is a cyber intelligence sharing community that focuses on financial services.
[16] The Office of Management and Budget (OMB) Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 2017), defines a breach as "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (a) an individual other than the authorized user accesses or potentially accesses PII [Personally Identifiable Information], or (b) an authorized user accesses or potentially accesses PII for an other than authorized purpose."
[17] JPMorgan Chase and Company, Current Report (Form 8-K) (October 2, 2014). According to the company, information compromised in the breach consisted primarily of customer contact information, such as names, addresses, phone numbers, and email addresses, as well as internal company information pertaining to the bank's customers.
[18] The BSA, 31 USC 5311 et seq., is sometimes referred to as an anti-money laundering (AML) law, or jointly as BSA/AML. Money laundering involves masking the source of criminally derived proceeds so they appear legitimate, or masking the source of monies used to promote illegal conduct.

For example, in January 2021, Capital One, N.A. admitted to willfully failing to implement and maintain an effective AML program to guard against money laundering and was assessed a $390 million civil monetary penalty.[19] Similarly, Banamex USA (BUSA) admitted to failing to maintain an effective AML compliance program to guard against money laundering and failing to file Suspicious Activity Reports (SARs).[20] BUSA agreed to forfeit $97.44 million for BSA violations, and the FDIC and California Department of Business Oversight ordered BUSA to pay a $140 million civil money penalty to resolve separate BSA regulatory matters.

Terrorist Financing. In October 2015, the Financial Action Task Force (FATF)[21] issued a report, entitled *Emerging Terrorist Financing Risks*. According to this report, the banking sector remains an attractive means for terrorist groups seeking to move funds globally because of the speed and ease at which they can move funds within the international financial system. The report states that the sheer size and scope of the international financial sector provides terrorist groups and financiers the opportunity to blend in with normal financial activity to avoid attracting attention.

Natural Disasters. According to a DHS *Homeland Threat Assessment* (October 2020), natural disasters encompass all types of environmental and severe weather hazards, including hurricanes, floods, earthquakes, tornadoes, wildfires, and winter storms. In 2020, many insured financial institutions faced staffing, utility, telecommunications, and other disruptions as a result of Hurricane Laura and the California wildfires.[22] In September 2017, Hurricane Maria caused significant property damage to the Commonwealth of Puerto Rico, St. Croix, and the U.S. Virgin Islands, and seriously impacted the operations of insured financial institutions in these areas.[23] Such natural disasters prompted the FDIC to highlight options available to financial institutions affected by declared federal emergencies, and consider regulatory relief from certain filing and publishing requirements.

Climate change has also emerged as a potential threat to U.S. financial stability. In November 2020, the Financial Stability Board (FSB) reported that climate risks could

[19] FinCEN News Release entitled *FinCEN Announces $390,000,000 Enforcement Action Against Capital One, National Association for Violations of the Bank Secrecy Act*, January 15, 2021.
[20] Department of Justice News Release, entitled *Banamex USA Agrees to Forfeit $97 Million in Connection with Bank Secrecy Act*, May 22, 2017.
[21] FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
[22] *Interagency Statement on Supervisory Practices Regarding Financial Institutions Affected by Hurricane Laura and California Wildfires* (September 2020) issued by the FDIC, the OCC, the Federal Reserve Board, the NCUA, and state banking regulators.
[23] See FDIC Financial Institution Letter (FIL), entitled *REGULATORY RELIEF: Guidance to Help Financial Institutions and Facilitate Recovery in Areas Affected by Hurricane Maria* (FIL-46-2017, September 2017).

"amplify credit, liquidity and counterparty risks and challenge financial risk management in ways that are hard to predict."[24] Additionally, the Financial Stability Oversight Council has identified climate-related financial risk as a priority.[25]

Pandemics. In January 2020, the World Health Organization declared the outbreak of a novel coronavirus—Coronavirus Disease (COVID-19)—a global health emergency. The World Health Organization defines a pandemic as the worldwide spread of a new disease. The Financial Stability Oversight Council's (FSOC)[26] Annual Report for 2020 described the global pandemic caused by COVID-19 as "the biggest external shock to hit the post-war U.S. economy."

Sources of Threat Information

There are numerous sources of threat information pertinent to the safety and soundness of financial institutions. Sources of threat information used by the FDIC to support supervisory activities include the following:

- News outlets, social media sites, blogs, bulletin boards, and other forums available to the general public. These "open sources" provide information about all types of threats that could impact insured financial institutions.

- Cyber threat information services offered by commercial vendors. These commercial vendors collect information about cyber threats, including those that could impact insured financial institutions, from many sources across the global landscape.

- The Financial and Banking Information Infrastructure Committee (FBIIC). Chartered under the President's Working Group on Financial Markets, the FBIIC has responsibility for improving coordination and communication among financial regulators, enhancing the resiliency of the Financial

[24] FSB report, entitled *The Implications of Climate Change for Financial Stability* (November 2020). The FSB is an international organization that promotes financial stability by coordinating with national financial authorities and international standard-setting bodies. The Vice Chairman for Supervision of the Federal Reserve Board chairs the FSB, through a non-renewable term that will end in 4Q2021, and the FSB's U.S. plenary members are the Federal Reserve Board the Securities and Exchange Commission (SEC) and the Treasury Department. The FDIC participates in FSB activities.
[25] Treasury Department News Release entitled *Remarks by Secretary of the Treasury Janet L. Yellen on the Executive Order on Climate-Related Financial Risks,* May 20, 2021.
[26] The Dodd-Frank Act created FSOC. FSOC's responsibilities include identifying threats to the financial stability of the United States, promoting market discipline, and responding to emerging risks to the stability of the United States financial system.

Services Sector, and promoting public-private partnerships. The Federal agency members of the FBIIC operate pursuant to a Memorandum of Understanding under which they share non-public cyber threat information pertaining to financial institutions.[27]

- The Federal Financial Institutions Examination Council (FFIEC). The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. The FFIEC created the Cybersecurity and Critical Infrastructure Working Group (CCIWG) to enhance communication among the FFIEC member agencies and build upon existing efforts to strengthen the activities of other interagency and private sector groups. The FFIEC's CCIWG coordinates with intelligence, law enforcement, Homeland Security, and industry officials to assist financial institutions in protecting themselves and their customers from the risk posed by cyber-attacks.

- The Treasury Department and its component organizations.

    - The Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) coordinates the Treasury Department's efforts to enhance the security and resilience of Financial Services Sector critical infrastructure and reduce operational risk. OCCIP works with financial sector companies, industry groups, and government partners (including the FDIC and other FBIIC member agencies) to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents.

    - The Office of Intelligence and Analysis (OIA) has responsibility for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of the Treasury Department. OIA analyzes

[27] The Federal agency members are the FDIC, the OCC, the NCUA, the Federal Reserve Board, the Treasury Department, the CFPB, the SEC, the Commodity Futures Trading Commission, the Farm Credit Administration, and the Federal Housing Finance Agency. The stated purpose of the MOU is to (a) identify, assess, mitigate, and develop a common situational awareness of incidents, threats and related vulnerabilities affecting any element of the Financial Services Sector; (b) cooperate on information-sharing issues; and (c) collaborate on any other matter within FBIIC's purview related to the operation of the Financial Services Sector, including but not limited to operational resilience.

financial intelligence to identify illicit financial activities, including those in the banking sector.

- The Treasury Department's Financial Crimes Enforcement Network (FinCEN) has responsibility for safeguarding the U.S. financial system from money laundering, terrorist financing, and other illicit activities. FinCEN collects and analyzes financial transaction information provided by financial institutions.[28] FinCEN also issues public and non-public advisories to insured financial institutions concerning money laundering and terrorist financing threats.

- The Treasury Department's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions programs based on U.S. foreign policy and national security goals. OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, countries subject to sanctions. OFAC also lists individuals, groups, and entities, such as terrorists and narcotics traffickers. The FDIC evaluates the effectiveness of programs at insured financial institutions designed to ensure that they do not provide banking services to such sanctioned entities identified by OFAC.

- The Department of Homeland Security (DHS). DHS supports the Treasury Department and Federal regulators (including the FDIC) by providing analysis, expertise, and technical assistance to critical infrastructure owners and operators, and conducting vulnerability assessments, among other things. CISA, a component within DHS, provides the government and private sector entities, including the FDIC and insured financial institutions, with threat information to protect against evolving cyber risks. Within CISA, the National Cybersecurity and Communications Integration Center serves as a central location where the FDIC and other Federal agencies, state, local, tribal, and territorial governments, and the private sector (including international stakeholders) coordinate efforts on cybersecurity.

- The Federal Bureau of Investigation (FBI). The FBI disseminates information regarding specific threats to entities, including insured financial institutions, through various methods, including Private Industry Notifications (PINs) and

[28] Financial institutions operating in the United States, including insured banks, must file SARs with FinCEN when the institution detects a possible violation of law or regulation, such as money laundering or terrorist financing. FinCEN makes SAR filings available to the FDIC for its analysis.

FBI Liaison Alert System (FLASH) reports.[29] The FBI also works with industry partners in forums such as InfraGard[30] and the Financial Services Information Sharing and Analysis Center (FS-ISAC)[31] to share threat information.

- FS-ISAC. FS-ISAC disseminates and fosters the sharing of relevant and actionable threat information to entities, including insured financial institutions, in the financial services industry. FS-ISAC shares this information with 16,000 users located in more than 70 countries. FS-ISAC obtains financial threat information by monitoring open source websites and private sources of information for relevant and actionable cyber and physical threat, vulnerability, and attack data.

- Insured financial institutions and their service providers. These entities must report certain types of threats, such as suspected terrorism and money laundering, in SAR filings with FinCEN. Insured financial institutions must also report incidents that involve a compromise of customer information to their primary Federal regulator. In addition, FDIC examinations, such as IT and BSA/AML examinations, can identify threats to financial institutions.

[29] PINs provide information intended to enhance the private sector's awareness of a threat, and FLASH reports contain technical information collected by the FBI for use by specific private sector partners.
[30] InfraGard is a public-private partnership between the FBI and tens of thousands of private sector members that represent all 16 critical infrastructure sectors.
[31] FS-ISAC serves as the operational arm of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The mission of the FSSCC is to strengthen the resilience of the Financial Services Sector against attacks and other threats to the Nation's critical infrastructure by proactively identifying threats, promoting protection, driving preparedness, collaborating with the U.S. Federal government, and coordinating crisis response.

- The Intelligence Community. Members of the Intelligence Community consist of executive branch agencies and organizations that engage in intelligence activities necessary for the conduct of foreign relations and the protection of national security.[32] The Office of the Director of National Intelligence leads the Intelligence Community, and its members collect, analyze, produce, and disseminate national intelligence,[33] including intelligence relevant to insured financial institutions and the Financial Services Sector.

  The FDIC is not a member of the Intelligence Community. However, according to an assessment report prepared by DOA for the FDIC Chairman, Board of Directors, and senior management, "[i]t has been determined that classified information[34] exists in Intelligence Community channels that would help FDIC with internal programs as well as executing its core mission specifically with regard to anti-money laundering, bank secrecy, economic espionage, threat finance, financial systems critical infrastructure protection (CIKR), cyber threat (both internal to FDIC corporate and external to banks and service providers), insider threat, foreign visitors to FDIC, and executive decision support."[35] The FDIC receives sensitive unclassified and classified National Security Information from the Intelligence Community to build situational awareness of threats and support policy and operational decision-making.

[32] Title 50 of the United States Code governs the intelligence activities of the United States and identifies the 18 members of the Intelligence Community. 50 U.S.C. § 3003. The FDIC is not a member of the Intelligence Community.
[33] According to the *National Intelligence Strategy of the United States of America 2019*, the term, "national intelligence," means "all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director [of National Intelligence], to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security."
[34] Classified information consists of marked or unmarked information, including oral communications, classified under the standards of Presidential Executive Order 13526, *Classified National Security Information* (December 2009), or under any other Executive Order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination.
[35] Assessment report, entitled *FDIC: SCIF Justification and National Security Information (NSI) Strategic Assessment* (June 2013).

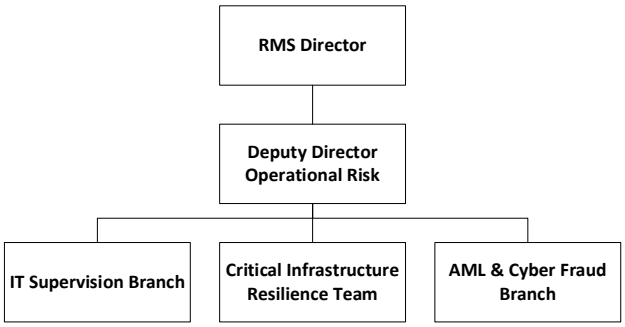
Roles and Responsibilities of FDIC Components

Several component offices within the FDIC play roles in acquiring, analyzing, and disseminating threat information to support the supervision program.

RMS Operational Risk Group

In 2016, the FDIC established the RMS Operational Risk group. One of the group's functions is to identify, monitor, analyze, and share information about operational risks that can threaten the safety and soundness of FDIC-supervised financial institutions. As shown in Figure 2, the Operational Risk group consists of two branches and a Critical Infrastructure Resilience Team.

Figure 2: The RMS Operational Risk Group



Source: OIG analysis of RMS Organizational Charts.

IT Supervision Branch

The IT Supervision Branch provides regulatory policy and guidance on IT and other operational risk-related matters, and oversight of financial institutions and technology service providers. To accomplish its mission, the IT Supervision Branch develops and maintains IT examination policy and guidance, including the IT Risk Examination (InTREx) Program.[36] The IT Supervision Branch is responsible for identifying and addressing emerging operational and information technology risks through research and supporting the examination process that promotes the safety and soundness of financial institutions.

Critical Infrastructure Resilience Team

The Critical Infrastructure Resilience Team serves as advisors to RMS management on cybersecurity and critical infrastructure-related issues to facilitate RMS and financial sector preparedness and resilience. The team researches, assesses, and disseminates operational threat information affecting the banking sector, financial institutions, and their service providers. The Team coordinates with the Treasury

[36] The FDIC, in coordination with the Federal Reserve Board and state bank regulators, developed the InTREx Program in July 2016 to support IT and operations risk examinations of state-chartered financial institutions.

Department, CISA, and other public- and private-sector organizations to obtain relevant information on threats. Senior Examination Specialists on the Critical Infrastructure Resilience Team often represent the FDIC on the FBIIC (in addition to the Deputy Director), and on the FFIEC CCIWG.[37]

AML and Cyber Fraud Branch

The AML and Cyber Fraud Branch develops rules and establishes policies, guidance, procedures, and relationships to address and identify risks, such as cyber fraud, money laundering, terrorist financing, and other illicit financial activities. To accomplish its mission, the AML and Cyber Fraud Branch establishes examiner training, conducts outreach to the banking industry and public, and coordinates with FinCEN, OFAC, law enforcement agencies, and other entities to acquire and share threat information.

The RMS Operational Risk group generates various types of written products and communications that contain threat information. These include a weekly *Cybersecurity Brief*, a bi-weekly *RMS Cybersecurity and Critical Infrastructure Protection Update*, a *Quarterly Operational Risk Book*, and ad hoc *Advisory Bulletins* covering various threats, such as COVID-19, terrorism, and ransomware. The Operational Risk group disseminates these products and communications to supervisory personnel in Headquarters and examination staff in the Regional and Field Offices for informational purposes. The Operational Risk group also shares threat information with the FDIC's Regional Risk Committees.[38]

The Intelligence Support Program

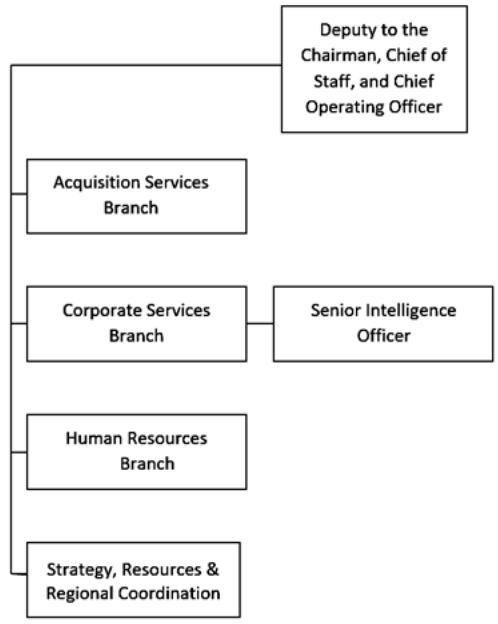
In April 2015, the FDIC hired its first Senior Intelligence Officer (SIO). The SIO initially worked in the Chief Information Officer Organization (CIOO) and reported directly to the Chief Information Security Officer. The SIO's responsibilities included coordinating the establishment of an "FDIC-wide strategic information and intelligence program and operations" and sharing of sensitive information both internally and with members of the Intelligence Community.

[37] Established in June 2013, the CCIWG serves as a liaison between the Financial Services Sector, Intelligence Community, law enforcement, and homeland security agencies regarding cybersecurity and critical infrastructure efforts.

[38] The FDIC has established Risk Committees in each of its Regional Offices to assess existing and emerging risks and key trends affecting financial institutions, service providers, and the financial industry. Each Regional Risk Committee produces a report in the spring and fall that describes relevant risks and trends and corresponding supervisory strategies. The Regional Risk Committee reports include information about threats affecting the banking industry, such as cyber attacks, money laundering, terrorist financing activities, and the pandemic.

In June 2016, the FDIC transferred the SIO function to the Division of Administration's (DOA) Corporate Services Branch. Figure 3 illustrates the SIO's organizational placement within DOA. Following the transfer, the FDIC expanded the SIO responsibilities to include "leading and managing the FDIC-wide comprehensive, all-hazards intelligence support program and its functions." The Intelligence Support Program was intended to provide FDIC executives and staff with accurate and timely all-source intelligence with the potential to impact the FDIC and the Financial Services Sector. Such intelligence includes all operational hazards (except natural disasters)[39] from both foreign and domestic sources.

Figure 3: Organizational Placement of the Senior Intelligence Officer



Source: OIG analysis of DOA Organizational Charts.

The SIO works with FDIC personnel to determine the types of threat information they need to support their programs, operations, and business decisions. The SIO records this information in an *Information Needs Document*. The SIO tailors the *Information Needs Document* to inform the intelligence community regarding the priorities and activities of the FDIC's Intelligence Support Program on issues relevant to FDIC stakeholders. The SIO also shares the *Information Needs Document* with members of the Intelligence Community to inform them of the FDIC's intelligence requirements. The Intelligence Community may consider the FDIC's needs, along with the intelligence requirements of other entities, when developing the National Intelligence Priorities Framework.

The SIO acquires threat information by conducting research and coordination with personnel in DHS, the Treasury Department, the Intelligence Community, and other public and private sector organizations. The SIO analyzes the information collected from these sources and shares it with FDIC stakeholders through written

[39] Personnel in DOA's Corporate Services Branch and RMS' Critical Infrastructure Resilience Team handle threat information involving natural disasters.

communications and in-person briefings. FDIC stakeholders use this threat information to build situational awareness and support business decision-making.

In February 2018, the FDIC designated the individual serving as the SIO to serve as the FDIC's Federal Senior Intelligence Coordinator (FSIC).[40] Intelligence Community Directive 404, *Executive Branch Intelligence Customers* (July 2013), states that the FSIC is a senior position within executive branch departments and agencies designated to serve as the primary liaison with the Intelligence Community. As the FDIC FSIC, the SIO coordinates all requests for information from the Intelligence Community with personnel throughout the FDIC. The FSIC also manages the review and approval of Intelligence Community credentials for FDIC employees in order to access secure facilities at Federal departments and agencies.

FDIC Users of Threat Information

The FDIC uses threat information to maintain situational awareness of threats and risks and to support business decisions.

Executive Leadership

Senior FDIC executives, such as the FDIC Chairman, the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff, and Division and Office Directors use threat information to maintain situational awareness of significant threats and risks to the FDIC and its personnel, insured financial institutions and their service providers, and the Financial Services Sector. Executive leadership also uses threat information to support policy development and business decision-making.

Supervisory Personnel

RMS personnel in Headquarters use threat information to maintain situational awareness of threats affecting insured financial institutions, their service providers, and the Financial Services Sector. These Headquarters personnel also use threat information to help shape supervisory policy, procedures, strategies, guidance, and training, and to conduct reviews and assessments of insured financial institutions at a national level. In certain cases, Headquarters

[40] See the former Chief Operating Officer's letter to the Deputy Director, Federal State and Local Partnerships, Office of the Director of National Intelligence, dated February 5, 2018. The SIO had served as the FDIC's Acting FSIC from March 2016 to February 2018. The FDIC's former CISO held the role of FSIC from April 2014 to March 2016. The FDIC's former CIO held the role of FSIC prior to the CISO.

personnel share threat information directly with insured institutions, which in turn may use the information to implement risk mitigation actions.

Examiners in the Regional and Field Offices may use threat information to maintain situational awareness of threats pertaining to the financial institutions they supervise. Examiners also may use threat information to develop institution-specific supervisory strategies, allocate resources, perform risk assessments, scope examinations, influence examination findings, and monitor risks and trends.

CISR personnel in Headquarters and the Regional Offices may use threat information to support the identification, monitoring, and assessment of risks at LCFIs. LCFIs maintain extensive international operations, diversified business lines, large branch networks, substantial IT systems, and millions of depositor accounts. As such, LCFIs are subject to a wide range of threats from foreign adversaries, including cyber attacks, money laundering, terrorist financing, geopolitical tensions, civil unrest, and government sanctions. Threat information may provide CISR personnel with situational awareness of threats affecting LCFIs and facilitates effective monitoring for LCFIs.

Other FDIC Personnel

Many other FDIC Divisions and Offices may use threat information to support their operations, programs, and business decisions, for example:

- The CIOO and the Office of the Chief Information Security Officer may use cyber threat information to identify and mitigate risks to the FDIC network, information systems, and data.

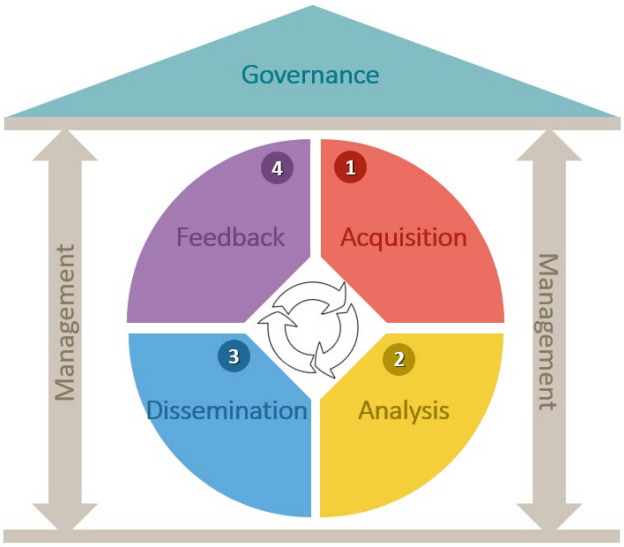
- Because cyber incidents have the potential to threaten the viability of insured financial institutions, the Division of Resolutions and Receiverships may need information about cyber threats so it can prepare accordingly for potential resolutions.

- The DOA Security and Emergency Preparedness and Crisis Readiness and Response Section may use threat information to: (i) conduct personnel security reviews; (ii) address physical security risks facing FDIC facilities, personnel, equipment, and information; (iii) support its Insider Threat and Counterintelligence Program activities; (iv) mitigate supply chain risks in FDIC procurements; and (v) prepare for crises readiness.

Processes for Sharing Threat Information

Based on our review of relevant Federal and private-sector plans, guidance, and practices,[41] we determined that the FDIC's threat sharing activities can be organized into four principal life cycle components: (1) acquiring relevant and actionable threat information from internal and external sources; (2) analyzing threat information to determine how it can support FDIC programs, operations, and decision-making; (3) disseminating threat information to stakeholders who need it; and (4) obtaining feedback from stakeholders regarding the utility of threat information and how threat information sharing processes can be improved.

Figure 4: The Threat Sharing Framework



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

In addition, the Government Accountability Office (GAO), OMB, and private sector organizations have published standards, guidance, and practices associated with successful program and project management.[42] These standards, guidance, and practices include elements of effective Governance, such as policies and procedures, roles and responsibilities, and goals and objectives. They also include elements of effective Management, such as succession and contingency planning, employee training, and information security risk management. Figure 4 illustrates

[41] These plans, guidance, and practices included DHS *Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community* (DHS Threat Framework) (October 2016); DHS *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*; DHS and the Treasury Department *Financial Services Sector-Specific Plan 2015;* and practices employed by other Federal agencies and industry organizations.

[42] GAO's *Standards for Internal Control in the Federal Government* (September 2014) (Internal Control Standards); OMB Memorandum M-18-19*, Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA)* (June 2018); OMB Circular A-11, *Preparation, Submission, and Execution of the Budget* (August 2021); the Project Management Institute's *The Standard for Program Management* (Fourth Edition, 2017); and industry publications on program and project management.

the four life cycle components of threat sharing, and their relationship to Governance and Management.

According to the GAO's Internal Control Standards, internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of an entity. The Internal Control Standards represent the minimum requirements for establishing effective internal controls at Federal agencies. The Federal Managers' Financial Integrity Act of 1982 (FMFIA) directs GAO to develop the Internal Control Standards, and FMFIA requires Federal executive branch agencies to implement them.[43] According to OMB Circular A-123, *Management's Responsibility for Internal Control* (December 2004), agency management has a fundamental responsibility to develop and maintain effective internal controls.[44]

AUDIT RESULTS

We found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The FDIC acquired, analyzed, and disseminated threat information to support the supervision of financial institutions. However, we identified gaps in each component of the Threat Sharing Framework. Specifically, the FDIC did not:

- Establish a written governance structure to guide its threat information sharing activities;
- Complete, approve, and implement a governance Charter that established a common understanding of the role of the Intelligence Support Program or defined an overall strategy and requirements;
- Develop goals, objectives, or measures to guide the performance for its Intelligence Support Program;
- Establish adequate policies and procedures that defined roles and responsibilities for key stakeholders involved in the threat information sharing program and activities; and

[43] The FDIC is not directly subject to FMFIA. However, it is the FDIC's practice to consider the guidance set forth in the GAO Internal Control Standards.
[44] OMB Circular A-123 provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations and meeting the requirements of FMFIA.

- Ensure that it had fully considered the risks identified in this report for its Enterprise Risk Inventory and Risk Profile.

We also identified gaps in the FDIC's processes for acquiring, analyzing, and disseminating threat information, and in its processes for obtaining feedback from stakeholders regarding how the use of threat information can be improved.

- **Acquisition.** The FDIC did not engage all relevant stakeholders when it developed its *Information Needs Document* that contains the FDIC's threat information requirements. As a result, the FDIC has limited assurance that it will acquire all relevant threat information to support its business operations and programs. In addition, current Federal regulations do not require prompt reporting of destructive cyber incidents that could threaten the safety and soundness of insured financial institutions unless the incident involves sensitive customer information. Reporting of destructive cyber incidents that do not involve sensitive customer information would provide the FDIC and other Federal bank regulators vital information needed to effectively assess threats and implement timely supervisory actions.

- **Analysis.** The FDIC did not establish procedures to guide its analysis of threat information. Absent such procedures, the FDIC relied solely on the discretion of certain individuals to determine the extent to which additional threat information should be analyzed to support FDIC's business needs and the supervision of financial institutions. Without procedures, the FDIC has limited assurance that the threat analysis it performs is consistent and sufficient to address the needs of stakeholders. Procedures would also help to ensure a smooth transition of knowledge to new analysts when staff depart the FDIC. Further, expanding the scope and depth of threat analysis could provide the FDIC with more effective threat information.

- **Dissemination.** The FDIC did not develop policies or procedures for disseminating threat information within the FDIC. Absent such procedures, decisions regarding the dissemination of threat information were left solely to the discretion of individuals, which could lead to inconsistent or untimely communications. In addition, the FDIC required its Regional Directors to hold high-level security clearances, so these personnel could access classified information in the performance of their duties. However, we found that the Regional Directors rarely or never received classified information and the FDIC had not established an infrastructure that would allow for the secure handling of such information to the regional offices. Such infrastructure includes the systems and protocols for the secure dissemination,

transmission, communication, use, storage, and disposition of classified information.

- **Feedback.** The FDIC did not establish a procedure to obtain feedback from recipients of threat information to assess its utility and effectiveness. Such structured feedback could provide valuable information regarding the extent to which FDIC personnel use threat information to build situational awareness and influence supervisory decision-making.

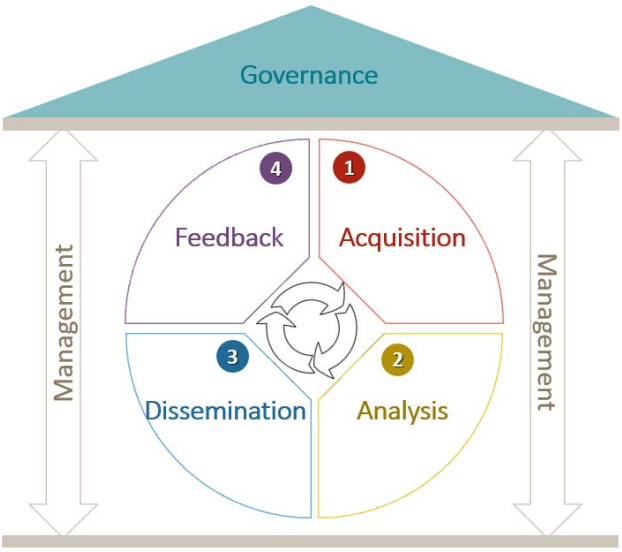
We also identified weaknesses in the FDIC's management control activities. Specifically, the FDIC did not establish an alternate (backup) for its SIO position, or develop a succession plan to mitigate the risk of a prolonged absence or departure of the SIO. Since April 12, 2021, the SIO has been serving on a detail assignment and the FDIC has not named a replacement to fill this position.

In addition, the FDIC did not establish minimum training requirements for the SIO position to ensure the continued development and retention of knowledge, skills, and abilities. Further, the FDIC did not take action to obtain required security clearances for two of its six Regional Directors until we identified the exceptions during this audit. Finally, the FDIC did not categorize unclassified threat information managed by the SIO consistent with security standards and guidance issued by the NIST.

GOVERNANCE OF THREAT INFORMATION SHARING ACTIVITIES

The Project Management Institute's (PMI) publication, entitled *The Standard for Program Management*,[45] states that program governance comprises the framework, functions, and processes by which a program is monitored, managed, and supported in order to meet organizational strategic and operational goals. Well-designed program governance provides practices for effective decision-making and ensures organizations manage programs appropriately. According to the PMI, effective program governance

Figure 5: The Threat Sharing Framework: Governance



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

- Ensures that program goals remain aligned with the strategic vision, operational capabilities, and resource commitments of the sponsoring organization;

- Facilitates the engagement of program stakeholders by establishing clear expectations for each program's interactions with key governing stakeholders throughout the program;

- Creates an environment for communicating and addressing program risks and uncertainties to the organization, as well as opportunities and issues that arise during the course of program performance; and

[45] PMI has conducted extensive research and analysis in the field of program and project management and has 652,000 members in over 100 countries worldwide. PMI is an American National Standards Institute (ANSI) accredited standards developer. One of ANSI's roles is to bridge the gap between the standards community and the government agencies that issue regulations or establish voluntary programs affecting them. Over 70 government agencies or departments, at both the Federal and state level, are members of the ANSI federation. The FDIC's CIOO has adopted PMI standards to guide its IT projects. PMI's *The Standard for Program Management* (Fourth Edition, 2017) provides guidance on principles, practices, and activities of program management that are important to program success and generally recognized to support good program management practices.

- Provides a framework that aligns with portfolio and governance policies and processes for assessing and ensuring program compliance. Each program may need to create a particular governance process or procedure, but it should align with the organization's governance principles.

When organizations do not maintain effective governance over their programs, it can lead to negative results, such as processes and activities that do not align with the organization's mission or strategic goals and objectives, and services that do not satisfy stakeholder needs.

The FDIC did not establish adequate governance to guide its threat sharing activities. Specifically, the FDIC did not complete, approve, or implement a Charter that established a common understanding of the role of the Intelligence Support Program or defined an overall strategy and requirements. The FDIC also had not developed goals and objectives for this program and did not address the acquisition, analysis, or dissemination of threat information under the Intelligence Support Program. In addition, the FDIC did not establish policies or procedures that defined roles and responsibilities for key stakeholders involved in threat information sharing. Further, the FDIC's Enterprise Risk Inventory did not capture many of the risks identified during the audit. The FDIC should ensure that its Enterprise Risk Profile and Risk Inventory fully considers the risks discussed.

Threat Information Sharing Activities Not Governed by a Charter

PMI's *The Standard for Program Management* states that many organizations prepare documented descriptions for their programs' governance frameworks, functions, and processes. These documented descriptions, which *The Standard for Program Management* refers to as a Charter, define the vision, mission, purpose, scope, authorities, assumptions, constraints, risks, benefits, goals, objectives, success factors, and strategy for engaging stakeholders. According to *The Standard for Program Management*, documenting this information in a Charter facilitates the design and implementation of effective governance and helps to ensure that the program aligns with organizational strategic priorities.

In addition, one Federal banking regulator had documented its governance structure for acquiring, analyzing, and disseminating cyber threat information used to support the bank supervision function.[46] Specifically, this Federal regulator documented the mission, functions, organizational structure, roles and responsibilities, processes, workflows, communications protocols, analytical standards, products, and

[46] This Federal regulator provided information that was not authorized for public attribution.

performance measures associated with its cyber threat sharing activities. For example, this Federal regulator documented processes and workflows for 1) monitoring threat information sources; 2) analyzing inputs; 3) processing information to determine what reporting should be presented for approval and escalation; 4) documenting communications 5) conducting after-action reviews; and 6) evaluating recommendations for resources, training and policy and guidance.

Further, DHS published *the Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community* (October 2016). This DHS Framework describes the processes and mechanisms used to facilitate the flow of threat information between and among entities involved in critical infrastructure security and resilience.

FDIC Had Not Completed, Approved, or Implemented a Charter for the Intelligence Support Program

Almost three years ago, in August 2018, the SIO began drafting a *National Intelligence Program Charter* (Draft Program Charter) for its Intelligence Support Program to "establish a framework and policy governing the Federal Deposit Insurance Corporation (FDIC) national intelligence program and functions." The Draft Program Charter states that it will serve as "the official guidance for FDIC divisions and offices" with respect to:

- *The acquisition, analysis, de-confliction, and dissemination of U.S. Government (USG) and non-USG foreign and domestic intelligence and threat information;*
- *Engagement with the U.S. Intelligence Community;*
- *Setting intelligence and information need priorities; and*
- *Sharing FDIC information with the Intelligence Community.*

The Draft Program Charter described the purpose, scope, and background of the FDIC's Intelligence Support Program, and identified the statutory and policy authorities under which the program would operate. In addition, the Draft Program Charter defined roles and responsibilities for key stakeholders, such as the SIO, FSIC, RMS's Senior Cybersecurity and Critical Infrastructure Specialist, and the ITCIP Manager. In June 2021, the SIO updated the Draft Program Charter and presented it to FDIC management for review and approval. As of August 31, 2021, the updated draft charter was still under review.

Without an approved Charter that defines an overall strategy and requirements for acquiring, analyzing, and disseminating threat information under the Intelligence Support Program, there may not be a common understanding of the program's mission and purpose, and it will lack coordination and structure. The lack of a Charter increases the risk that FDIC stakeholders will not receive relevant, accurate, or timely information about threats to maintain situational awareness and make informed decisions. A Charter for the Intelligence Support Program would also provide clear, strategic direction for stakeholders, and help to ensure effective coordination among stakeholder organizations with similar threat information sharing responsibilities.

Recommendation

We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

1. Establish, approve, and implement a Charter to govern the acquisition, analysis, and dissemination of threat information under the FDIC's Intelligence Support Program.

Goals, Objectives, and Measures for Threat Information Sharing Activities Not Adequate

The GAO stated that performance goals and objectives, and related performance measures, serve as important management tools for planning Federal programs and initiatives.[47] According to the GAO, program goals and objectives communicate the results agencies seek for their programs. Performance measures demonstrate the progress agencies make toward achieving program goals and objectives. Performance measures provide agency managers with crucial information to identify gaps in program performance, and to plan any needed improvements. GAO's Internal Control Standards recognize performance goals and objectives and related measures as key components of an effective internal control system.
Each year, the FDIC develops annual FDIC Performance Goals (FPGs) to focus the agency's attention on fulfilling its core mission responsibilities and highest priority initiatives. We reviewed the FPGs established between 2019 and 2021 and

[47] For example, see GAO reports, entitled *Federal Buildings, GSA Should Establish Goals and Performance Measures to Manage the Smart Buildings Program* (Report No. GAO-18-200) (January 2018); *Performance Measurement and Evaluation: Definitions and Relationships*, (Report No. GAO-11-646SP) (May 2011); and *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, (Report No. GAO-05-927) (September 2005).

identified several FPGs that focused on improving the FDIC's ability to acquire, assess, and share threat information pertaining to financial institutions.[48] In addition, to FPGs, FDIC Divisions and Offices may also establish goals and objectives at a Division or Office level. We reviewed the Division-level goals established by RMS and DOA between 2019 and 2021 and identified several RMS goals that focused on improving the analysis and sharing of threat information with FDIC supervisory personnel.[49] At the close of our audit, as of July 2021, CISR had not established Division-level goals or objectives with respect to threat information sharing activities.

None of the FDIC FPGs or Division-level goals and objectives addressed the FDIC's Intelligence Support Program. According to the SIO, the FDIC has not established goals or objectives for the Intelligence Support Program over the past six years, since 2015.[50] In addition, DOA's Division-level goals covered a wide range of priorities and initiatives, including ones related to the FDIC's Insider Threat and Counterintelligence Program.[51] However, none of DOA's Division-level goals addressed the Intelligence Support Program or its threat information sharing responsibilities.

The FDIC also had not developed performance measures that would allow it to assess the performance of threat sharing activities under its Intelligence Support Program. The *National Strategy for Information Sharing and Safeguarding* issued by the President in December 2012 recommends that Federal departments and agencies measure improvements in information sharing and safeguarding processes, including how shared information helps to achieve department and agency missions.

Without performance goals and objectives, and related measures, the FDIC cannot effectively measure the performance of its threat information sharing activities.

---

[48] For example, the FDIC established FPGs to: (1) improve the analysis and sharing of cybersecurity threat information with financial institutions; (2) implement a computer security incident notification final rule for insured financial institutions; (3) research and consider the potential impact of climate change on the financial sector; and (4) expand cyber and IT supervisory expertise to better analyze and assess IT and cybersecurity risks in LCFIs.

[49] For example, RMS established priorities to: (1) conduct two webinars through the FFIEC on current operational threats and methods for addressing them; and (2) mature capabilities for delivering information and actionable threat information to applicable stakeholders within RMS and CISR.

[50] In 2015, the FDIC established FPGs to (1) develop an interdivisional framework to identify and address rising cybersecurity risks in the Financial Services Sector and (2) increase the FDIC's representation and communication within the Federal Intelligence Community by (among other things) hiring an SIO and developing and implementing standard operating procedures for cyber threat and incident sharing.

[51] *The Insider Threat and Counterintelligence Program (ITCIP) Governance Charter and Implementation Plan* (September 2016) and the *FDIC Insider Threat and Counterintelligence Program (ITCIP) Concept of Operations* (March 2017) also define strategic goals and performance metrics for the ITCIP.

Further, without evidence-based performance information, the FDIC's ability to make informed decisions about how to improve its threat information sharing processes and activities is limited. The lack of performance goals and objectives, and related measures, pertaining to the FDIC's Intelligence Support Program was a contributing factor in the weaknesses identified during the audit such as a lack of procedures to guide analysis of threat information, and a lack of succession planning for key threat sharing roles.

In March 2021, DOA management and the SIO prepared a presentation for the FDIC's Deputy to the Chairman, Chief Operating Officer, and Chief of Staff. The presentation included a proposal to adopt performance goals and measures to mature the Intelligence Support Program. The SIO made this presentation and proposal several months after we raised concerns with FDIC management about a lack of performance goals and objectives and related measures. As of August 30, 2021, FDIC management had not adopted any performance goals and measures for the Intelligence Support Program.

According to the GAO, setting goals and objectives and measuring performance is a leading practice of results-oriented organizations. Establishing and implementing performance goals and objectives, and associated measures, instill accountability in Federal programs and initiatives, and promote transparency regarding management's expectations for results.

Recommendation

We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

2. Establish and implement performance goals, objectives, and measures to govern and assess the threat sharing activities performed under the FDIC's Intelligence Support Program.

FDIC Policies and Procedures on Threat Information Sharing Activities Lacking

GAO Internal Control Standards state that organizations should document policies that define responsibilities for achieving operational process objectives and addressing related risks. According to the Internal Control Standards, individuals serving in key roles may further define policies through day-to-day procedures. The Internal Control Standards state that organizations should periodically review their policies and procedures to ensure that they are relevant and effective. Policies and

procedures serve as an important control for ensuring that processes are repeatable, consistent, and disciplined, and for reducing operational risk associated with changes in staff. Policies and procedures also communicate management's directives to employees and help to ensure that employees properly carry out those directives.

We found that the FDIC did not develop written policies or procedures to govern the acquisition, analysis, or dissemination of threat information under the FDIC's Intelligence Support Program. In addition, we found that although RMS developed procedures to acquire, analyze, and disseminate information about cyber incidents at FDIC-supervised financial institutions and their service providers, RMS did not review and update these procedures regularly (at least annually) to ensure that they were current. Further, RMS did not develop procedures to guide its efforts to acquire, analyze, or disseminate threat information in support of the supervision program.

Inadequate Policies and Procedures for the Intelligence Support Program

The SIO has responsibility for developing and implementing effective, long-term, sustainable strategic intelligence support policies consistent with the FDIC's mission requirements. The SIO also has responsibility for updating and maintaining standard operating procedures for executing program activities. However, FDIC management did not provide the necessary direction for the SIO to develop written policies or procedures for acquiring, analyzing, or disseminating threat information under the Intelligence Support Program.

Inadequate Policies and Procedures in Supporting the Supervision Program

The SIO conducts research of classified and unclassified information to acquire relevant information about potential threats to insured financial institutions and the Financial Services Sector. The SIO analyzes and disseminates this information with RMS supervisory personnel in Headquarters to promote situational awareness of threats and to inform RMS decision-making. For example, the SIO acquires and analyzes classified information in support of background investigations conducted by RMS of foreign nationals listed on applications for Federal Deposit Insurance and Notices of Change in Control.[52] This work aims to identify information that may pose a threat to insured financial institutions or the Deposit Insurance Fund. Such threats may include, for example, a foreign national's affiliation with a foreign government

[52] Applications involve individuals or entities seeking to establish an insured financial institution. Notices involve individuals or entities seeking control of FDIC-supervised financial institutions and/or influencing their operations, such as serving as senior executive officers, directors, principal shareholders.

(including a foreign intelligence service) or involvement in money laundering, terrorist financing, or other illicit activities.

The SIO acquires threat information on foreign nationals by accessing classified information systems in the FDIC's Sensitive Compartmented Information Facility (SCIF).[53] The SIO also contacts personnel in the Treasury Department's Office of Intelligence and Analysis to determine whether they have any relevant information for which the SIO does not have access. The SIO then analyzes the information collected and shares the results with RMS personnel in the Operational Risk group. Although RMS has developed policies and procedures for conducting background investigations of individuals (including foreign nationals) listed on applications and notices,[54] the RMS procedures do not:

- Reference the role of the SIO in supporting the background investigation process for foreign nationals, including the scope and breadth of classified research permitted to be performed by the SIO;

- Identify the FDIC personnel authorized to request classified research of foreign nationals, or how such requests should be recorded. RMS officials and the SIO stated that such requests are often made verbally and not documented;

- Define the extent to which the SIO's research of classified information on foreign nationals is subject to supervisory review. The FDIC had not established any requirements for documenting the supervisory review or approval of the SIO work products;

- Establish protocols for sharing the results of the SIO classified research of foreign nationals; and

- Describe the manner in which classified materials supporting background investigations of foreign nationals must be organized and stored, and the period for which such information must be retained.

[53] The NIST defines a SCIF as an area, room, group of rooms, buildings, or installation certified and accredited as meeting the Director of National Intelligence security standards for the processing, storage, and/or discussion of as Sensitive Compartmented Information. The FDIC's SCIF contains classified information systems that allow authorized personnel to access, analyze, and share classified information to promote situational awareness of threats and to support management decision-making.
[54] See FDIC *Applications Procedures Manual*, Section 1.5, *Background Investigations*, and RMS Regional Directors Memorandum, *Background Investigations Policy and Procedures*, (Transmittal No. 2020-010-RMS, April 2020).

Establishing policies and procedures to govern highly sensitive activities, such as the SIO's acquisition, analysis, and dissemination of classified information in support of RMS background investigations, protects the FDIC's business interests. Specifically, policies and procedures help to ensure that the individuals performing sensitive activities understand the limits of their authority, and perform their duties in compliance with relevant laws, regulations, Executive Orders, and Federal guidance.

Figure 6: Example of Why Policies and Procedures for Intelligence Support Program are Needed

In March 2015, a former Counterintelligence Officer working in DOA determined that an FDIC contractor employee presented a potential insider threat because the employee had traveled to South Asia. In the absence of policies or procedures, the Counterintelligence Officer requested that various FDIC component organizations, including the OCISO, begin acquiring information about the employee's background and activities on the FDIC network. The FDIC's former CISO became concerned about the Counterintelligence Officer's efforts to acquire this information about a contractor employee without policies and procedures to guide the sensitive activities. The former CISO informed senior FDIC management of the concern.

In April 2015, the former FDIC Chairman, former Chief Operating Officer, and other senior FDIC executives met with DOA management and emphasized the need for policies and procedures and a governance structure to guide the acquisition, analysis, and sharing of sensitive threat information about FDIC and contractor employees. These senior executives directed DOA management to coordinate with the FDIC's Legal Division and CIOO to develop the policies, procedures, and a governance structure. Thereafter, DOA management instructed the former Counterintelligence Officer to discontinue counterintelligence activities until policies, procedures, and a governance structure were established.

In July 2016, the former Acting FDIC Inspector General testified during a Congressional hearing that the lack of policies and procedures delayed the implementation of the FDIC's ITCIP, [55] and further disclosed this information in a letter to a member of Congress in December 2016.[56] The FDIC formally established policies and procedures for its ITCIP in September 2016.

Figure 6 illustrates how a lack of policies and procedures over threat information sharing activities delayed the implementation of the FDIC's ITCIP in 2015.

[55] *Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?*, U.S. House of Representatives, Committee on Science, Space, and Technology, July 14, 2016.
[56] Letter from Acting FDIC Inspector General to the Honorable Suzanne Bonamici, U.S. House of Representatives (December 8, 2016).

The FDIC's Legal Division can provide expertise in evaluating the legal authorities and limitations, as well as in developing policies and procedures to guide threat information sharing activities under the Intelligence Support Program.

Inadequate Policies and Procedures for SIO Serving as the Federal Senior Intelligence Coordinator

The SIO serves as the FDIC's Federal Senior Intelligence Coordinator (FSIC). According to Intelligence Community Directive 404, *Executive Branch Intelligence Customers* (July 2013), the FSIC serves as the primary liaison between executive branch departments and agencies and the Intelligence Community. As such, the FDIC FSIC coordinates all requests for information from the Intelligence Community with personnel throughout the FDIC and works with FDIC personnel to ensure consistent responses to these requests. The FSIC also manages the review and approval of Intelligence Community Badges for FDIC employees. As of January 22, 2021, [redacted] FDIC employees held Intelligence Community Badges.

The FDIC had not developed policies or procedures that defined the responsibilities of the FSIC. Such policies and procedures are important because they help to ensure that FDIC personnel understand their obligation to coordinate with the FSIC when addressing requests from the Intelligence Community. Such policies and procedures also help to ensure that the SIO, acting as the FSIC, properly manages requests and approvals for Intelligence Community Badges and that a continued business need exists for active badges.[57] Proper management of Intelligence Community Badges helps to ensure that access to highly secure government facilities is properly controlled.

Inadequate Policies and Procedures for Developing the FDIC's Threat Information Needs

The SIO works with FDIC personnel to determine the types of threat information they need to support their programs, operations, and business decisions. The SIO records this information in an *Information Needs Document*.[58] The SIO uses the *Information Needs Document* as a baseline set of requirements for the information that the FDIC seeks to acquire. The *Information Needs Document* helps to prioritize the SIO efforts to address the threat issues most relevant to FDIC stakeholders.

[57] FDIC Directives 1610.01, *Physical Security Program* (August 2021), and 1600.8, *Personal Identity Verification (PIV) Card Program* (July 2017), address FDIC-issued identification badges, but not Intelligence Community Badges.

[58] The SIO maintained two versions of the *Information Needs Document*—a classified version and an unclassified version. We reviewed the unclassified version. According to SIO, there are minimal differences between classified and unclassified versions.

The SIO also shares the *Information Needs Document* with members of the Intelligence Community to inform them about the type of information that the FDIC seeks to acquire. The Intelligence Community considers the FDIC *Information Needs Document*, along with the intelligence requirements of other entities, when developing the National Intelligence Priorities Framework. The Director of National Intelligence uses the National Intelligence Priorities Framework to establish the intelligence priorities for the Nation.

The FDIC had not developed policies or procedures for developing, approving, or maintaining the *Information Needs Document*. In addition, the *Information Needs Document* did not capture the information requirements of all relevant FDIC Division and Office stakeholders. For example, the *Information Needs Document* did not capture requirements for CISR, DRR, or the Regional Directors. Without knowing the needs of these stakeholders, the FDIC cannot be sure that it will obtain relevant threat information needed to inform supervisory decision-making. Further, the FDIC did not subject the *Information Needs Document* to senior supervisory review and approval.

Inadequate Procedures in the RMS Operational Risk Group

The RMS Operational Risk group acquires and analyzes information about threats that can affect insured financial institutions, their service providers, and the Financial Services Sector. The Operational Risk group incorporates this threat information into various written products that it disseminates to supervisory staff in Headquarters, examination staff in the Regional and Field Offices, and personnel in CISR who monitor LCFIs. Such products include a weekly RMS *Cybersecurity Brief*; periodic RMS *Advisory Bulletins* covering various threats such as COVID-19, terrorism, and ransomware; the Treasury Department monthly *Financial Sector Cyberthreat Trends* report; and RMS *Quarterly Operational Risk Book* covering cyber fraud, financial crimes, money laundering, and other types of threats. However, RMS did not review and update its cyber incident response procedures regularly (at least annually) to ensure they remained current, or develop procedures to guide the acquisition, analysis, or dissemination of threat information.

Cyber Incident Response Procedures

The RMS cyber incident response procedures consist of two component documents:

- The *RMS Regional Cyber Incident Response Guide*. This Guide contains procedures that RMS Regional and Field Office personnel must follow to: gather and record relevant information about incidents; evaluate incident

severity, including whether incidents warrant escalation to Headquarters; monitor incident remediation; and close incidents.

- The *RMS Cyber Incident Response Plan* (CIRP). The CIRP outlines procedures that Headquarters personnel must follow to: assess the severity of incidents (based on systemic risk and impact); escalate incidents within RMS and communicate them to other stakeholder Divisions and Offices; and share incident information with outside parties, such as the FBIIC.

We reviewed the CIRP in June 2020 to determine whether it contained current information regarding the FDIC incident response processes and practices. The CIRP states that it "shall be reviewed annually and updated as necessary." We found that RMS had not updated the CIRP since October 2016. As a result, portions of the CIRP did not contain current information. Specifically, the CIRP

- Identified the FDIC Intelligence and Critical Infrastructure Protection Committee as a governance body involved in incident notifications and threat sharing; however, the FDIC dissolved this governance body in 2018;

- Identified key point of contact personnel who had either retired from the FDIC or transferred to different positions;

- Did not reflect the organizational re-alignment implemented by the FDIC in July 2019 that created CISR; and

- Referenced an outdated RMS policy and defunct FDIC Outlook email box for sharing incident information.

In August 2020, we informed RMS management that components of the CIRP were outdated. In February 2021, the RMS Director re-issued the CIRP to reflect current processes.

Inadequate RMS Procedures for Acquisition, Analysis, and Dissemination of Threats

RMS did not develop procedures that defined roles, responsibilities, or processes for

- Identifying relevant sources of threat information, or monitoring and gathering information from those sources;

- Analyzing threat information and generating the various types of written products that contain threat information;

- Identifying relevant and actionable threat information that needs to be disseminated, determining which stakeholders need this information and how it will be communicated (verbally, in writing); and ensuring threat information is disseminated in a timely manner.

Another Federal Banking Regulator had developed written roles, responsibilities, and operating procedures for acquiring, analyzing, and sharing cyber threat information in support of its bank supervision program.

Without current and up-to-date policies and procedures, threat information sharing activities are left solely to the discretion of individuals, which may lead to inconsistent decisions and practices in sharing threat information. Policies and procedures help to ensure that threat information sharing activities occur in a repeatable and consistent manner.

According to the GAO Internal Control Standards, documentation of internal controls, such as policies and procedures, "provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel." This reduces operational risk associated with staff turnover and departures. For example, if the SIO unexpectedly departed the FDIC, a successor may find it difficult to readily implement key threat information sharing duties and responsibilities.

In addition, policies and procedures communicate management's directives and expectations to employees, and help to ensure that employees understand and properly carry out those directives and expectations. This is particularly important for employees performing highly sensitive activities, such sharing classified threat information. Further, policies and procedures help to hold individuals accountable should they fail to comply with management's directives and expectations.

Recommendations

We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer coordinate with the FDIC Legal Division to:

3. Establish and implement policies and procedures that define roles and responsibilities for acquiring, analyzing, and disseminating threat information under the FDIC's Intelligence Support Program.

4. Establish and implement policies and procedures governing the use of national intelligence to conduct background investigations of foreign nationals listed on applications for Federal Deposit Insurance and Notices of Change in Control.

5. Establish and implement policies and procedures to govern the activities of the FDIC Federal Senior Intelligence Coordinator.

6. Establish and implement policies and procedures for developing, approving, and maintaining the *Information Needs Document*.

We recommend that the Director, RMS, coordinate with the Legal Division to:

7. Define roles and responsibilities for RMS threat information sharing activities.

8. Establish and implement procedures for RMS threat information sharing activities.

Threat Information Sharing Weaknesses Not Fully Considered as Enterprise Risks

OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular A-123, July 2016), requires Federal agencies to implement an Enterprise Risk Management (ERM) capability.[59] According to OMB Circular A-123, ERM is an effective agency-wide approach to addressing the full spectrum of an organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos.

FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (October 2018), establishes policy, responsibilities, and key components for a comprehensive ERM and internal control program. According to this Directive, each FDIC Division and Office is responsible for identifying its key activities and determining what risks may threaten the FDIC's ability to achieve success.

The FDIC's Chief Risk Officer (CRO) and Office of Risk Management and Internal Controls (ORMIC)[60] maintain the Risk Inventory to capture the enterprise risks identified by the FDIC's Divisions and Offices. FDIC Divisions and Offices have responsibility for keeping the Risk Inventory updated throughout the year, and for

[59] The FDIC has determined that OMB Circular A-123 is not binding on the FDIC with respect to ERM. However, FDIC Directive 4010.3 states that the FDIC "does embrace the spirit of ERM as outlined in OMB Circular A-123.

[60] On December 15, 2020, the Deputy to the Chairman and Chief Financial Officer announced an organizational change. Effective January 1, 2021, the FDIC reorganized the former Risk Management and Internal Controls Branch within the Division of Finance and elevated it to a separate, independent office known as ORMIC.

conducting an annual, Agency-wide validation. The Risk Inventory informs the development of a prioritized list of the most significant risks facing the FDIC, known as the Risk Profile. The FDIC *Enterprise Risk Management Standard Operating Procedure* (May 2021) states that the FDIC identifies risks through Division and Office risk assessments; audits and evaluations conducted by the OIG and GAO; FDIC risk committees; and research and risk assessments performed by ORMIC. The ERM SOP further states that the FDIC assesses all risks facing the Agency, including inherent and residual risks, and considers existing control mitigations that reduce inherent risks.

We reviewed the FDIC's Risk Inventory and found that it did not include risks related to the lack of an Intelligence Support Program governance Charter; goals, objectives, and measures; policies and procedures; and management controls such as training requirements and contingency plans for the SIO and security clearances for key personnel. Addressing these risks will require coordination among multiple component business units within the FDIC.

Without an enterprise view of the risks, the FDIC may not acquire all relevant threat information, effectively analyze threat information to create actionable products, disseminate those products to all appropriate stakeholders in a timely manner, or obtain feedback from recipients to continually improve threat information sharing processes. Moreover, if the FDIC does not provide relevant, actionable, and timely threat information to all relevant stakeholders, its operations, programs, and decision-making may be negatively affected.

Accordingly, the risks warrant review from an enterprise perspective for the Risk Inventory and Risk Profile. Integrating risk management practices across functional lines, rather than addressing risks within silos, is a focus of the FDIC's ERM program and helps to ensure a consistent approach in the assessment and remediation of risks.

Recommendation

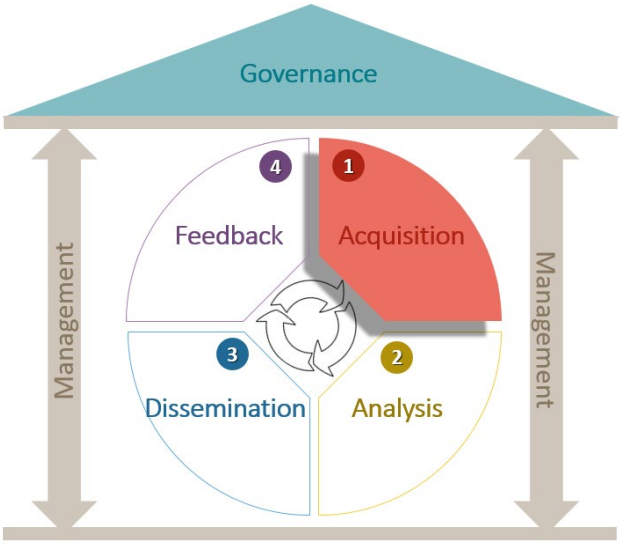
We recommend that the Chief Risk Officer:

9. Ensure that FDIC Enterprise Risk Inventory and Risk Profile fully consider the threat information sharing risks identified in this report.

ACQUISITION OF THREAT INFORMATION

According to GAO's Internal Control Standards, management should design a process to identify the information requirements needed to achieve the entity's objectives and address risks. Based on its information requirements, management should obtain all relevant data from reliable internal and external sources in a timely manner. Further, the *2012 National Strategy for Information Sharing and Safeguarding* stated that informed decision-making requires the ability to discover, retrieve, and use accurate, relevant, timely, and actionable information.

Figure 7: The Threat Sharing Framework: Acquisition



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

The FDIC has established agreements and working relationships with various Federal departments, agencies, and outside organizations to acquire threat information to support the supervision of FDIC-supervised financial institutions.[61] The FDIC also routinely monitored "open source" and classified channels to acquire threat information.

However, the FDIC did not develop written procedures for determining its threat information requirements. In addition, the FDIC did not engage all relevant stakeholders when it developed its *Information Needs Document*, which articulates the FDIC's threat information requirements. If the FDIC does not adequately define its threat requirements, it may not acquire all relevant threat information to support its business operations and programs.

[61] Such agreements include, for example, a Memorandum of Understanding with members of the FBIIC (November 2020) to facilitate the sharing of information involving incidents, threats, and vulnerabilities affecting the Financial Services Sector and the *FFIEC Crisis Communication Protocols* (December 2016) that define a framework for how members of the FFIEC coordinate on significant threats, vulnerabilities and incidents impacting financial institutions under their supervision.

Further, existing Federal regulations do not require prompt reporting of destructive cyber incidents that could threaten the safety and soundness of insured financial institutions. Requiring such reporting would provide the FDIC and other Federal bank regulators vital information needed to effectively assess threats and implement timely supervisory actions.

Threat Information Needs Not Fully Defined

The Intelligence Support Program's SIO works with FDIC personnel to determine the types of threat information needed to support FDIC programs, operations, and business decisions. For example, the SIO coordinated with personnel in the RMS Operational Risk group to determine how the SIO's access to classified and unclassified information could facilitate the assessment of threats affecting insured financial institutions.

The SIO records identified threat information requirements in an *Information Needs Document*.[62] The *Information Needs Document* serves as a baseline set of requirements for the information that the FDIC seeks to acquire to support its programs, operations, and decision-making. The *Information Needs Document* also helps to prioritize the SIO's efforts to address the issues most relevant to FDIC stakeholders.

However, coordination with FDIC Division and Office stakeholders was informal and not guided by written procedures. We found that the Intelligence Support Program did not incorporate input from CISR, Regional Directors, and DRR in the *Information Needs Document*. For example:

- The Intelligence Support Program did not meet with representatives of CISR to discuss how foreign threat information could support CISR monitoring and resolution planning for LCFIs. LCFIs maintain extensive international operations, diversified nonbank business lines, large branch networks, substantial IT systems, and millions of depositor accounts. Thus, LCFIs are subject to a wide range of threats from foreign adversaries, such as cyber attacks, money laundering, terrorist financing, geopolitical tensions, civil unrest, and government sanctions.

[62] The SIO maintained two versions of the *Information Needs Document*—a classified version and an unclassified version. We reviewed the unclassified version. According to the SIO, there were minimal differences between the classified and unclassified versions. The primary difference between these two versions was that the classified version aligned the FDIC's threat information requirements with the National Intelligence Priorities Framework.

The SIO stated that discussions with CISR personnel would likely identify foreign threat information that could enhance CISR's awareness of threats affecting LCFIs. CISR personnel stated that they did not have access to classified threat information that could affect the institutions they monitor. CISR officials acknowledged that the SIO's access to threat information could help to inform CISR's situational awareness of threats and the effectiveness of its monitoring of LCFIs.

- The Intelligence Support Program did not coordinate with FDIC Regional Directors to determine their threat information needs. The Regional Directors have direct responsibility for assessing operational threats affecting insured financial institutions in their respective regions.

- The Intelligence Support Program did not coordinate with representatives from DRR to determine its threat information needs. Threat information can support effective resolution planning. For example, a cyber threat could be severe enough to cause insured financial institutions to fail. The more informed DRR is about threats that can jeopardize the safety and soundness of institutions, the more effectively it can plan for potential resolutions.

If the *Information Needs Document* does not address all relevant requirements, FDIC stakeholders may not receive the information that they need to support their programs, operations, and decision-making. In addition, the FDIC did not subject the *Information Needs Document* to senior supervisory review and approval. Such supervisory review and approval helps to ensure that work is performed in accordance with internal control standards and applicable legal and regulatory requirements. Supervisory review and approval also helps to ensure that work products contain current, accurate, and complete information.

Recommendation

We recommend that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff:

10. Update and approve the *Information Needs Document* to incorporate input from all relevant Divisions and Offices regarding their threat information requirements.

Financial Institutions Not Required to Promptly Report Destructive Cyber Threats

In February 2001, the Federal bank regulators promulgated *Interagency Guidelines Establishing Information Security Standards* (Interagency Guidelines) in the Code of Federal Regulations (CFR).[63] The Interagency Guidelines establish standards for developing and implementing safeguards to protect the security, confidentiality, and integrity of customer information. The Interagency Guidelines, and supplemental guidance published by the Federal bank regulators,[64] state that every financial institution should develop and implement a Response Program "to address incidents of unauthorized access to customer information in customer information systems."[65] According to the Interagency Guidelines and supplemental guidance, an institution's Response Program should include procedures for "notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information." This reporting requirement also applies when an incident occurs at an institution's service provider.

However, the scope of the Interagency Guidelines and supplemental guidance extends only to incidents that compromise customer information. Federal regulations do not address reporting to Federal bank regulators other types of destructive cyber incidents that could jeopardize the safety and soundness of an institution. Such incidents include, for example, denial-of-service attacks and ransomware attacks that can disrupt an institution's operations and inflict severe and potentially irreversible damage to information systems and data.

In November 2015, the FFIEC issued a joint statement wherein it encouraged financial institutions to notify their primary Federal regulator when they become a victim of a destructive cyber attack.[66] However, such notifications are not required.

In addition, our analysis of cyber incident data maintained by the FDIC found that FDIC-supervised institutions did not report cyber incidents in a prompt manner. We reviewed 226 cyber incidents reported by financial institutions between January 2017

[63] The FDIC Interagency Guidelines for the entities subject to its jurisdiction are codified at 12 CFR Part 364, App. B and 12 CFR Part 391, subpart B, App. B.
[64] See *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 12 C.F.R. Part 364, App. B (Supp. A). The FDIC, the OCC, the Federal Reserve Board, and the former Office of Thrift Supervision issued this supplemental guidance to interpret the requirements of section 501(b) of the Gramm-Leach-Bliley Act and the Interagency Guidelines.
[65] FDIC regulations define customer information as any record containing non-public personal information about a customer that is maintained by or on behalf of the institution. 12 CFR Part 364.
[66] See *FFIEC Joint Statement, Cyber Attacks Involving Extortion* (November 2015).

and June 2020 and determined that it took an average of 87 days for the institutions to report the incidents to the FDIC.[67]

- In one incident, the FDIC learned that a financial institution was victimized by ransomware during a risk management examination. The examination occurred approximately 3 months after the ransomware attack took place.

- In another incident, the FDIC became aware that a financial institution was victimized by ransomware through an analysis of SARs filed with the Treasury Department's FinCEN. The FDIC conducted the SAR analysis approximately 4 months after the ransomware attack occurred.

While risk management examinations and SARs can provide valuable information about cyber attacks, they are not designed to ensure timely notification to the FDIC about incidents affecting the safety and soundness of insured institutions. In addition, financial institutions have up to 30 calendar days to file a SAR following the initial detection of facts triggering a SAR filing requirement.[68] The SAR filing deadline may be extended an additional 30 days (up to a total of 60 calendar days) if available information does not identify a suspect. Also, the FDIC generally conducts risk management examinations of financial institutions every 12 or 18 months,[69] potentially allowing many months to pass between a cyber attack incident and an examination.

OIG Advisory Memorandum Issued to FDIC Management

On April 30, 2020, we issued an Advisory Memorandum to FDIC management describing our concerns about existing regulations which did not require insured

[67] The FDIC maintained cyber incident data in its [redacted] system. The 226 incidents we reviewed consisted of 102 Crimeware incidents, 94 Web application attacks, and 30 denial-of-service attacks. We calculated the 87 days by measuring the elapsed time between the date the institution discovered the incident to the date the FDIC entered the incident into [redacted]. FDIC management expects FDIC staff to enter incidents into [redacted] when they become aware of the incidents. Crimeware is a type of malicious software designed to carry out or facilitate illegal online activity and includes ransomware.

[68] Under the reporting requirements of BSA and its implementing regulations, insured financial institutions must file SARs when they detect a known or suspected criminal violation of Federal law or a suspicious transaction related to a money-laundering activity.

[69] Section 337.12 of the FDIC Rules and Regulations that implement Section 10(d) of the FDI Act requires an annual full-scope examination of every insured state nonmember bank at least once during each 12-month period. Section 337.12 permits the FDIC to extend the annual examination interval to 18 months under certain conditions.

financial institutions to promptly report destructive cyber incidents.[70] Our Advisory Memorandum stated that establishing a Federal requirement for the prompt reporting of destructive cyber incidents could provide the FDIC and other Federal bank regulators more consistent information to assess threats and implement supervisory actions in a timely manner. On May 21, 2020, the FDIC responded, indicating that it would coordinate with other Federal bank regulators to develop a rule to address our concerns about banks not having to report destructive cyber incidents.[71]

On December 18, 2020, the Federal bank regulators jointly announced issuance of a notice of proposed rulemaking entitled, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*. The proposed rule would require banking organizations (referred to herein as financial institutions) to provide their primary Federal regulator with prompt notification of any computer-security incident[72] that rises to the level of a notification incident.[73] The proposed rule would also require such notification as soon as possible, but no later than 36 hours after a financial institution believes in good faith that an incident has occurred.

Under the proposed rule, service providers also would be required to notify affected customers of financial institutions immediately after the service provider experiences a computer-security incident that it believes could disrupt, degrade, or impair the provision of financial services. In addition, the proposed rule would require service providers to contact affected financial institutions to help ensure they comply with the notification requirements. The FDIC established a Performance Goal for 2021 to implement the computer security incident notification rule.

[70] See Appendix 3 for the OIG's Advisory Memorandum, entitled *Cybersecurity Incident reporting by Insured Financial Institutions* (April 2020).
[71] See Appendix 3 for management's response to our Advisory Memorandum, entitled *Cybersecurity Incident reporting by Insured Financial Institutions* (May 2020).
[72] The Proposed Rule defines a computer-security incident as "an occurrence that results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." 86 Fed. Reg. 2299 (Jan. 12, 2021).
[73] The Proposed Rule defines a notification incident as "a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair: the ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or those operations of a banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States." 86 Fed. Reg. 2299 (Jan. 12, 2021).

Need for Prompt Reporting of Cyber Incidents

In February 2021, the FDIC updated its guidance for Regional Offices to follow when responding to cyber incidents at financial institutions or their service providers. The FDIC's *Regional Cyber Incident Response Guide* states that "[k]nowing about and responding to incidents at supervised entities is important to the FDIC mission." Information about cyber incidents enables the FDIC to effectively advise institutions affected by cyber incidents, drawing from the FDIC's experience in supervising other entities impacted by cyber incidents. Further, receiving cyber incident information allows the FDIC to conduct analysis across entities to improve supervisory guidance, adjust supervisory programs, and provide information to the industry to help entities protect themselves.

The Regional *Cyber Incident Response Guide* further recognizes that a cyber incident may so severely impact an institution's safety and soundness that it ultimately causes the institution to fail. The Guide states that the sooner the FDIC knows of such incidents, the better it can prepare for the institution's failure. Cyber incidents can disrupt information systems and compromise data in a matter of minutes. The potential severity and speed of a cyber incident could compress ordinary resolution planning timelines. Therefore, prompt reporting of destructive cyber incidents by financial institutions would facilitate the FDIC's resolution planning activities.

Prompt reporting of destructive cyber incidents also helps law enforcement officials, including criminal investigators working in the FDIC OIG, who investigate and pursue prosecution of malicious cyber actors. The Department of Justice cited "the value of early notification to law enforcement" in the recovery of bitcoins valued at approximately $2.3 million following a ransomware attack in May 2021 against Colonial Pipeline.[74]

Recommendation

We recommend that the Director, RMS:

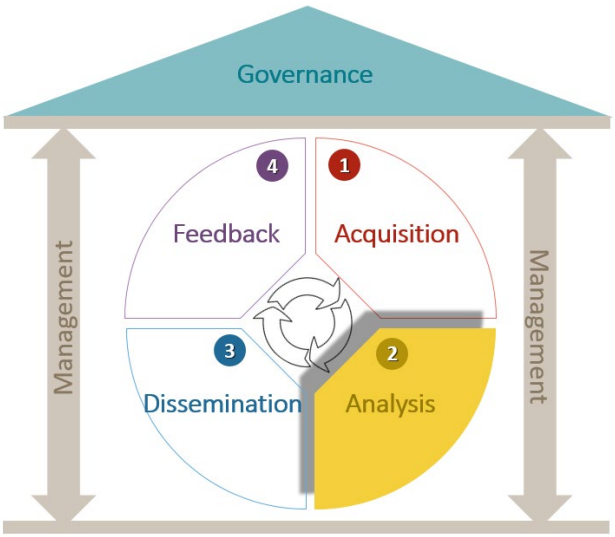
11. Finalize and implement a requirement for FDIC-supervised financial institutions to promptly report destructive cyber incidents to the FDIC.

[74] See *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 2021), issued by the U.S. Department of Justice, U.S. Attorney's Office for the Northern District of California.

ANALYSIS OF THREAT INFORMATION

GAO's Internal Control Standards state that management should analyze the risks it identifies so that it can prioritize responses to mitigate the risks. The Internal Control Standards also state that management may use various risk analysis methodologies due to differences in entity missions and other factors. In the context of threats, analysis involves evaluating information and data to identify patterns, trends, and emerging issues, as well as to understand the motives, targets, and behaviors of threat actors.

Figure 8: The Threat Sharing Framework: Analysis



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

We found that the SIO and personnel in the RMS Operational Risk group analyzed certain threat information they acquired to support the supervision of financial institutions. However, the FDIC did not establish procedures to guide this analysis. In the absence of such procedures, the FDIC relied solely on the discretion of individuals to determine whether threat information should be subject to analysis, and if so, the extent to which the information should be analyzed. This increased the risk that threat information would not be subject to analysis consistent with the FDIC's needs. Further, procedures would help to ensure a smooth transition of knowledge to new analysts when staff depart the FDIC.

One Federal bank regulator that we contacted during the audit had established standard operating procedures to guide its analysis of threat information.[75] This regulator developed standard operating procedures to guide the development of analytical products it generated on cyber-related issues, threats, trends, and developments. These standard operating procedures also addressed metrics, dashboards, and heat maps the regulator used to monitor industry-relevant cybersecurity events, incidents, and trends.

[75] The Federal regulators that we spoke with during the audit provided information that was not authorized for public attribution.

Representatives of another regulator stated that they were working to establish procedures for the cyber threat risk profiles the regulator was developing to identify root causes of threats and the likelihood they would occur at institutions under the regulator's supervision. This regulator's analysis included trending of reported incidents to inform priorities each year for examinations. For example, the regulator identified ransomware and third-party service provider due diligence as specific areas of focus for its examiners. Such analysis can provide examiners with situational awareness of emerging threats affecting financial institutions and result in actionable information to inform supervisory activities.

As discussed earlier in this report, the FDIC had not developed a governance framework for its threat information sharing activities, including an overall strategy and requirements; written policies and procedures; or goals, objectives, and measures. These gaps increase the risk that the analysis it conducts of threats will not be sufficient to meet its needs. They also increase the risk of inconsistency across analysts and an inefficient transition of duties to new employees. Without written procedures to guide its threat information sharing activities, decisions regarding what information to analyze and the extent of analysis to be performed are left solely to the discretion of individuals, which may lead to inconsistent decisions and practices.

Analysis Performed under the Intelligence Support Program

The SIO has responsibility for conducting analysis of threat information in support of the FDIC's mission. The SIO also has responsibility for "briefing FDIC executives and senior staff on specific trends and patterns in cyber security, terrorism, emergency preparedness, foreign financial policies and activities, and other applicable strategic intelligence." Further, the SIO has responsibility for "preparing all-hazard threat assessments and threat briefs to senior FDIC officials relevant to the FDIC's mission."

Based on the FDIC's *Information Needs Document* and requests from FDIC stakeholders, the SIO analyzed threat information and shared the results through classified and unclassified briefings and written communications. For example, the SIO analyzed classified and unclassified foreign threat information acquired from numerous sources to prepare a weekly product for FDIC stakeholders called *The Global Intelligence Update*. *The Global Intelligence Update* described the potential impact of certain foreign threats on the FDIC, its personnel, and the U.S. Financial Services Sector.

The SIO analyzed threat information without written procedures to guide the level of depth (rigor and level of detail involved) or coverage (scope and breath) of analysis

performed. Such procedures could help to ensure that the SIO subjects threat Information to analysis in a consistent, timely, and objective manner, as well as in accordance with management's objectives, and stakeholder needs.

One Federal bank regulator had developed standard operating procedures that identified the standards its analysts adhere to when analyzing cyber threat information—Intelligence Community Directive 203, *Analytic Standards* (January 2015). The Office of the Director of National Intelligence issued Directive 203 to guide the analysis and production of analytic products across the Intelligence Community. Intelligence Community Directive 203 requires analytic products generated by the Intelligence Community to be consistent with five Analytic Standards.[76] We also noted that the FDIC had developed procedures for analyzing information under its Insider Threat and Counterintelligence Program.[77]

RMS Analysis of Threat Information

RMS officials informed us that the majority of threat information provided to RMS supervisory personnel in Headquarters and examiners in the Regional and Field Offices is acquired from sources outside the FDIC. Examples include the monthly *Financial Sector Cyberthreat Trends* report published by the Treasury Department, Emergency Directives and Alerts issued by CISA, and Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) reports issued by the FBI. In some cases, however, the RMS Operational Risk group summarizes analytical products prepared by others. For example, the RMS Operational Risk group produces a bi-weekly RMS *Cybersecurity and Critical Infrastructure Protection Update*; periodic RMS *Advisory Bulletins;*[78] and the RMS *Quarterly Operational Risk Book* covering cyber fraud, financial crimes, money laundering, and other types of threats.

[76] Intelligence Community Directive 203 states that analytic products must be: (1) Objective: analysts must perform their functions with objectivity and awareness of their own assumptions and reasoning; (2) Independent: analytic assessments must not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint; (3) Timely: analysis must be disseminated in time for it to be actionable by customers; (4) Based on all available sources: analysis should be informed by all relevant information available; and (5) Compliant with nine specific Analytic Tradecraft Standards that address such things as ensuring quality and credibility of underlying sources, data, and methodologies and addressing uncertainties associated with major analytic judgments. These standards are required to be followed by Intelligence Community agencies; however, there is no such requirement for non-Intelligence Community agencies such as the FDIC.

[77] These procedures are contained in the *FDIC Insider Threat and Counterintelligence Program (ITCIP) Concept of Operations* (March 2017) and the *FDIC Escalation and Triage Playbook* (July 2017).

[78] The RMS Operational Risk group issued three Advisory Bulletins during 2020 covering threats associated with ransomware, COVID-19, and terrorism. The RMS Operational Risk group issued two Advisory Bulletins during the first 6 months of 2021 covering threats associated with Microsoft Exchange Server and Pulse Connect Secure.

The RMS Operational Risk group maintained the threat information it handled in an internal shared platform accessible by hundreds of RMS and CISR personnel. The RMS Operational Risk group also detailed one of its employees to FinCEN on a part time basis to (among other things) analyze currency transaction reports and SARs to identify threats to the banking system.

However, the RMS Operational Risk group had not developed procedures to guide its analysis of threat information or the analytic products described above. A member of the RMS Operational Risk group stated that the Critical Infrastructure Resilience Team intends to perform expanded analysis of threat information to identify patterns, trends, or emerging issues that could be relevant to examiners in the field. Currently, the Critical Infrastructure Resilience Team reviews existing threat information it acquires from other sources to determine whether it needs to be shared with FDIC management, examiners in the field, or the banking industry.

We noted that the RMS Operational Risk group was not performing trend analysis of data collected by FDIC examiners regarding cyber attacks[79] against FDIC-supervised financial institutions and their service providers. Analyzing such information could identify the frequency, trend, type, location, and severity of cyber attacks. It could also help to identify the costs associated with the attacks[80] and their impact on earnings and capital, as well as the causes of the attacks.

For example, RMS's ViSION system contains IT examination data that could be useful for analysis such as information related to the types of incidents, time lapses between discovery and reporting, and information for critical incidents. In addition, the Regional Automated Document Distribution and Imaging system (RADD) stores electronic documents related to correspondence and other supervisory records that could possibly have value for threat analysis. Such analysis could be valuable to both policy makers and examiners in assessing cyber threats, formulating supervisory strategies, and evaluating the adequacy of InTREx procedures and examiner training.

[79] Cyber attacks include attacks such as ransomware, denial-of-service attacks, and web application attacks.
[80] Costs include, but are not limited to, ransom payments, the costs of hiring outside counsel and cybersecurity firms to assess and remediate the damage, cost to strengthen security controls, and lost business.

Recommendation

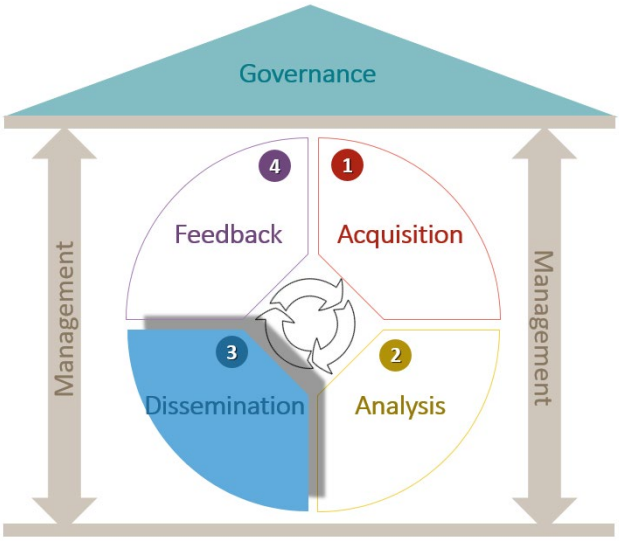
We recommend that the Director, RMS:

12. Ensure threat analysis includes relevant trends, patterns, and emerging issues facing financial institutions, including analysis of RMS data.

DISSEMINATION OF THREAT INFORMATION

The GAO Internal Control Standards state that "effective information and communication are vital for an entity to achieve its objectives." The Internal Control Standards state that agency management should have appropriate methods to communicate information based on the intended recipients, nature of the information, availability, cost and legal requirements.

Figure 9: The Threat Sharing Framework: Dissemination



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

For threat information to be actionable, it must be disseminated to the right people, in the right format, and at the right time. Policies and procedures help to ensure the effective dissemination of threat information to those who need it. Further, because threat information can be highly sensitive or classified, a proper infrastructure is necessary to allow for its secure dissemination. In addition, individuals receiving threat information must have the proper security clearance.

The RMS Operational Risk group and the SIO regularly disseminate threat information to supervisory personnel in Headquarters and the Regional and Field Offices through various channels, such as reports, emails, briefings, and conference calls. However, the FDIC did not develop procedures to guide the dissemination of this threat information. Absent such procedures, decisions regarding what to disseminate, to whom, and when are left solely to the discretion of individuals, which could lead to inconsistent or untimely communications.

In addition, the FDIC required its Regional Directors to hold high-level security clearances, so these personnel could access classified information in the performance their duties. However, we found that the Regional Directors rarely or never received classified information and the FDIC had not established an infrastructure that would allow for the secure handling of such information to the regional offices. Such infrastructure includes the systems and protocols for the secure dissemination, transmission, communication, use, storage, and disposition of classified information.

Regional Directors Did Not Receive Classified Information

Presidential Executive Order No. 13526, *Classified National Security Information* (December 2009), prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Executive Order 13526 defines three different levels of classified information as follows:

- **Confidential Information**, the unauthorized disclosure of which would cause "damage to the national security;"
- **Secret Information**, the unauthorized disclosure of which would cause "serious damage to the national security;" and
- **Top Secret (TS) Information**, the unauthorized disclosure of which would cause "exceptionally grave damage to the national security."

In addition, there is a category of classified information commonly associated with the TS level known as Sensitive Compartmented Information (SCI). According to DHS, SCI contains information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling within formal access control systems established by the Director of Central Intelligence.[81] Because of its elevated sensitivity, SCI requires special handling, need-to-know, and access restrictions that exceed those normally required for information at the same classification level.

In order to obtain access to classified information, individuals must first have a security clearance. A security clearance is a determination by a sponsoring Federal agency, that an individual is eligible for access to classified information.[82] There are three levels of security clearances that correspond to the three levels of classified information described above.

When an FDIC employee begins working in a position that requires a security clearance,[83] the employee's Division or Office must document a justification for the security clearance level on FDIC Form 1600/13, *Personnel Security Action Request*. The justification must describe the specific duties that require access to classified information. Divisions and Offices submit the completed Form 1600/13 to the DOA

[81] See DHS Management Directives System MD Number: 11043*, Sensitive Compartmented Information Program Management* (September 2004).
[82] *See* Congressional Research Service, *Security Clearance Process: Answers to Frequently Asked Questions* (October 2016).
[83] An employee's Position Description determines whether the position requires a security clearance.

Security and Emergency Preparedness Section (SEPS) for processing. FDIC Circular 1600.3, *National Security Program* (issued in September 2001 and updated in December 2017), states that SEPS has overall responsibility for processing and granting security clearances for FDIC personnel. If an employee also requires access to SCI, SEPS must request and obtain approval for SCI access from the FDIC's authorized investigative agency.[84]

Security Clearance Requirements for Regional Directors

The FDIC Position Description for the six Regional Directors requires that the individuals serving in these roles obtain and maintain a security clearance at the TS/SCI level. In July 2020, RMS cited several reasons why the Regional Directors would require access to classified information at the TS/SCI level, including the following:[85]

> *To make informed decisions, Regional Directors require situational awareness on threats that may impact the safety and soundness of financial institutions within their area of all responsibility. This threat information may come in the form of unclassified or classified data that may need to be briefed to executive decision makers. Classified data that Regional Directors may have a "need to know" may exist at the Secret or Top Secret levels with SCI access requirements.*
>
> *Regional Directors would be interacting with RMS executives at Washington Headquarters including the RMS Director and RMS Deputy Director Operational Risk as well as FDIC's Senior Intelligence Officer and RMS's Senior Specialists for Cybersecurity and Critical Infrastructure Protection. Regional Directors may also periodically be invited to attend classified briefings presented by the Financial and Banking Information Infrastructure*

[84] In January 2021, the OIG issued an evaluation report, entitled *The FDIC's Personnel Security and Suitability Program* (EVAL-21-001, January 2021). The report stated that the FDIC's Personnel Security and Suitability Program was not fully effective in ensuring that the FDIC: (1) completed preliminary background investigations in a timely manner; (2) ordered and adjudicated background investigations commensurate with position risk designations; and (3) ordered re-investigations within required timeframes. The report recommended that the FDIC strengthen the program's controls and ensure full compliance with Federal requirements. The report also recommended that the FDIC update policies and procedures, conduct additional training, and establish monitoring techniques to ensure the removal of individuals deemed unfavorable. In addition, the report recommended that the FDIC: (1) develop and implement a plan to ensure that it completes periodic reinvestigations in a timely manner; (2) correct system data and position risk inaccuracies; and (3) address background investigation weaknesses, including the development of metrics, reports, and monitoring for compliance with statutory requirements. The FDIC has addressed all of the report's recommendations.

[85] RMS justifications on FDIC Form 1600/13, *Personnel Security Action Request*.

Committee or ad hoc briefings presented by Federal law enforcement of [sic] the intelligence community.

Regional Directors may be required to review specific classified documents released to the FDIC by the intelligence or federal law enforcement community as well as internally generated monthly briefing documents derived from classified information.

Regional Directors have a need to know information, including threats against financial institutions that may impact the viability of that institution. That information may come in the form of classified intelligence. Such intelligence may be utilized to [sic] information decision making pertaining to resource allocation and risk-focusing of examination and supervisory-related activities.

Current briefings provided to FDIC executives are performed at TS/SCI, therefore SCI access would be required to participate in those briefings.

SEPS requires Divisions and Offices to certify periodically that their employees who hold security clearances continue to require them. Divisions and Offices complete these certifications on FDIC Form 1630/01, *Security Clearance Validation*. RMS submitted FDIC Forms 1630/01 to SEPS in May 2019 and again in October 2020 to certify that the Regional Directors had a continuing need for security clearances at the TS/SCI level to perform their duties.

Notwithstanding the documented need for the Regional Directors to have access to classified information at the TS/SCI level, all six Regional Directors stated that they had rarely or never received classified information. For example, the Regional Directors did not participate in classified briefings with RMS personnel, FBIIC, Federal law enforcement, or members of the Intelligence Community.

In addition, the Regional Directors did not receive classified information to inform their decision-making regarding resource allocations or the risk-focusing of examination and supervisory-related activities.

No Method to Share Classified Information with Regional Offices

A primary reason the Regional Directors did not receive classified information was because the FDIC had not established the necessary infrastructure to enable the dissemination or receipt of classified information in its regional office locations.

- The FDIC had neither established SCIFs in its Regional Offices nor made arrangements to use SCIFs controlled by other agencies near its Regional Offices.

- Three Regional Directors stated that they did not know whether a SCIF controlled by another agency was located near their office.

- The remaining three Regional Directors stated that a SCIF was located near their office, but they did not know whether the FDIC had made arrangements with the agencies controlling those SCIFs for FDIC personnel to use them.

Constructing and maintaining a SCIF involves a significant investment of financial resources. For this reason, agencies may choose to share a SCIF controlled by another agency to achieve efficiencies and cost savings.[86] Making arrangements to access a SCIF controlled by another agency in Regional Office locations would enable the FDIC to disseminate classified information to the Regional Directors. Establishing such access would be particularly important during a national emergency, such as a major cyberattack or terrorist event, when the FDIC may need to disseminate classified information to the Regional Directors in an urgent timeframe. Further, a national emergency could render the FDIC leadership and continuity of operations personnel unavailable or incapable of performing essential functions. Under this scenario, the FDIC may be required to devolve from its primary operating facilities in the National Capital Region to one or more of its Regional Office locations so essential business functions can continue. In the case of RMS, a Regional Director serves as the devolution successor to the RMS Director and would be required to serve in place of

> *Devolution occurs when an FDIC Division or Office temporarily transfers authority, responsibilities, and duties to another Division or Office in an un-impacted region to support the continuation of essential functions. The FDIC may devolve when its primary operating facilities and continuity site(s) become unavailable or are rendered inaccessible.*
>
> The FDIC Continuity of Operations Plan Version 2.0 (February 2020)

[86] The Intelligence Community refers to the practice of sharing SCIF space as "co-utilization." Under co-utilization arrangements, the "tenant agency" (the agency seeking access to a SCIF) establishes a written agreement (co-utilization agreement) with the "host agency" (the agency that controls the SCIF). The co-utilization agreement defines the purpose, nature, and responsibilities of the host and tenant agencies in sharing the SCIF. Co-utilization agreements can address such things as: protocols the tenant agency will follow when accessing the host agency's facilities and SCIF; the extent to which the tenant agency can use secured data networks and communications equipment in the host agency's SCIF; and the manner in which the tenant agency can store and dispose of classified materials and electronic data, such as briefing packages, presentations, and meeting notes, in the host agency's SCIF.

the RMS Director during a devolution. As discussed later in this report, we found that the specific Regional Director who would be next in line for succession (after the RMS Director) did not have the required security clearance. Without prior arrangements to access a SCIF, it would be difficult for the FDIC to rapidly disseminate classified information to the Regional Director during a devolution of the agency.

In addition to lacking a means to share classified information with the Regional Offices, we noted that only one individual in each Regional Office—the Regional Director—was required to hold a security clearance. If a Regional Director should become unavailable or leave his/her position unexpectedly, the FDIC would not have the ability to share classified information with anyone in that Regional Office. It is not clear how the Regional Directors could use this information to enhance supervisory programs because they would be prohibited from sharing the classified information with examiners who do not have a security clearance (or access to classified information), or anyone else in the Region.

Absent a method to share classified information within the Regional Offices (beyond those with appropriate security clearances), RMS personnel stated that they might be able to re-construct classified threat information into an unclassified form, by removing the classified portions. However, this approach would mean that the Regional Office personnel would not be receiving the complete information regarding the underlying threat, and it may lack the relevant context. In addition, such an approach would require time and effort by FDIC personnel, as well as a precise understanding of the classified portions and the reasons for the original classification. Further, it would necessitate that FDIC personnel have an expertise in modifying the original information into an unclassified form and may be subject to human error. This process may not be feasible or practical when information must be disseminated to a Regional Office (or Offices) in an urgent timeframe, such as a national emergency.

As described in the RMS justifications for their TS/SCI clearances, Regional Directors need access to classified information to carry out their supervisory responsibilities. Such responsibilities include maintaining situational awareness of threats impacting the safety and soundness of insured financial institutions, making informed decisions regarding resource allocations and supervisory strategies, and attending classified briefings and reviewing classified materials.

Recommendations

We recommend that the Director, RMS, and the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

13. Establish and implement a means to share classified information with the Regional Offices in a timely manner so that it is actionable.

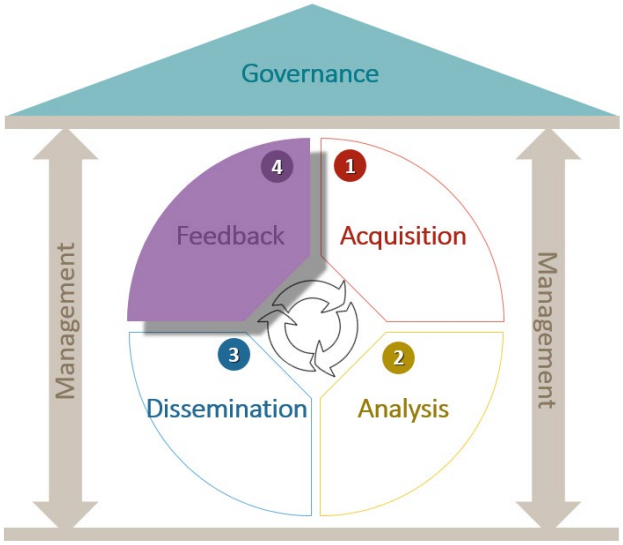
14. Establish a means for Regional Offices to handle classified information once it is shared, including the infrastructure (systems, facilities, and communications) to securely handle, transmit, discuss, store, and dispose of classified information.

15. Evaluate and document whether additional Regional Office personnel should be required to hold a security clearance based on business needs.

FEEDBACK FROM FDIC STAKEHOLDERS

The DHS *Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community* (October 2016) states that "an important component of the information-sharing cycle is the feedback recipients of the information provide to the originators and producers of analytic products to improve relevance, usefulness, and format." Such feedback allows originators and producers of threat information to adjust the volume, type, and timing of threat information to ensure the information remains effective in achieving its intended purpose. Further, GAO Internal Control Standards state that management should periodically review its control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks.

Figure 10: The Threat Sharing Framework: Feedback



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

The RMS Operational Risk group and the SIO disseminate threat information to supervisory personnel in Headquarters and examination staff in the Regional and Field Offices through recurring and ad hoc written products, briefings, conference calls, and other communications.

However, the FDIC has not established a procedure to obtain feedback from the recipients of this threat information to assess its utility and effectiveness in supporting supervisory activities and decision-making. Such structured feedback could provide valuable information regarding the extent to which FDIC personnel use threat information to:

- Build and maintain situational awareness of threats affecting insured financial institutions, their service providers, and the Financial Services Sector;
- Influence supervisory strategies, risk assessments, examination scoping, examination findings, and continuous monitoring activities; and

- Inform supervisory policy, guidance, and training programs.

We spoke with RMS personnel in all six Regional Offices to obtain their views on the utility and value of a threat-related product from the Operational Risk group—the weekly *Cybersecurity Brief*.

- RMS personnel in 3 of the 6 Regional Offices stated that the *Cybersecurity Briefs* contained information that was too voluminous to provide directly examiners. Individuals in these three Regional Offices review the *Cybersecurity Briefs* for relevant information, and then disseminate the information they deem relevant to examiners in the field.

- RMS personnel in 4 of the 6 Regional Offices stated that the *Cybersecurity Briefs* contained threat information of a general nature that was typically not actionable.

- RMS personnel in 5 of the 6 Regional Offices stated that the *Cybersecurity Briefs* contained information that Regional Office personnel had received through other sources, such as news articles and other government agencies.

A member of the RMS Operational Risk group stated that much of the information in the *Cybersecurity Briefs* is information that has already been reported by other organizations. This member acknowledged that examination staff in the Regional and Field Offices may already obtain the information in the *Cybersecurity Briefs* through other sources.

Further, we spoke separately with the SIO and learned that the FDIC has not established a procedure to obtain feedback from all Division and Office recipients of threat information shared through the FDIC's Intelligence Support Program.

Without a procedure to assess the utility and effectiveness of threat information, the FDIC may not provide threat information that recipients find relevant, actionable, and timely. As a result, the FDIC may not fully consider or assess all relevant threats as part of the supervisory process. Further, the FDIC may expend unnecessary resources to acquire, analyze, and disseminate threat information that is duplicative of information received from other sources.

Recommendation

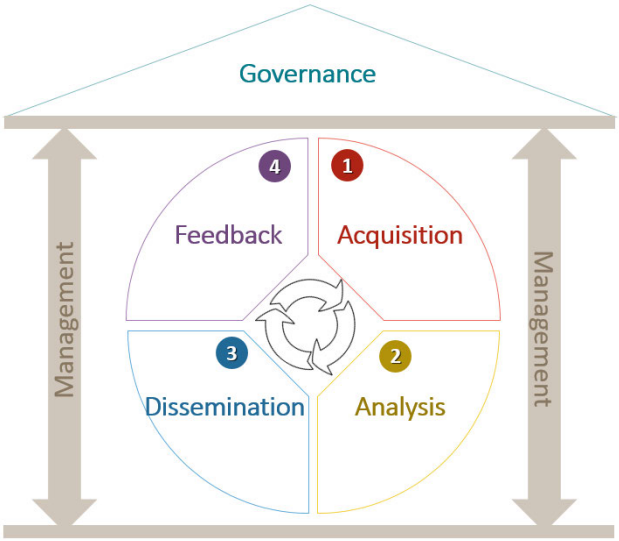
We recommend that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff and the Director, RMS:

16. Establish and implement a procedure to measure the utility and effectiveness of threat information used to support the supervision program.

MANAGEMENT OF THREAT INFORMATION SHARING ACTIVITIES

GAO Internal Control Standards define the minimum control activities that Federal agencies should implement to achieve their objectives and run their operations in an efficient and effective manner. These Management control activities include succession and contingency planning for individuals serving in key roles, professional training to ensure that employees have and maintain the competencies needed to effectively execute their duties, and security management practices to ensure the confidentiality, availability, and integrity of agency systems and data.[87]

Figure 11: The Threat Sharing Framework: Management



Source: OIG-developed Framework based on research of Federal and private-sector criteria.

We found that the FDIC did not:

- Establish an alternate (backup) for the SIO, or develop a succession plan to mitigate the risk of a prolonged absence or departure of the SIO. Since April 12, 2021, the SIO has been serving on a detail assignment and the FDIC has not named a replacement to fill this position.

- Establish minimum training requirements for the SIO position to ensure the continued development and retention of knowledge, skills, and abilities.

- Take action to obtain required security clearances for two of its six Regional Directors until we identified the exceptions during this audit.

[87] According to the Federal Information Security Modernization Act of 2014 (Public Law No. 113-283), confidentiality means "preserving authorized restrictions on [information] access and disclosure, including means for protecting personal privacy and proprietary information;" integrity means "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;" and availability means," ensuring timely and reliable access to and use of information."

- Categorize unclassified threat information managed by the SIO consistent with security standards and guidance issued by the NIST.

The Senior Intelligence Officer Did Not Have a Backup

GAO Internal Control Standards state that management should, as part of its human capital planning, consider how best to plan for the eventual departure of valuable employees and maintain continuity of needed skills and abilities. According to the Internal Control Standards, management should define contingency and succession plans for key roles to help ensure the entity continues to achieve its objectives. Contingency planning addresses the need to maintain continuity when a key individual is unavailable, or to respond to sudden changes in personnel, such as when an individual vacates a key role with little or no advance notice. Succession planning addresses the need to replace personnel over the long term.

The SIO is a key role with significant responsibility within the FDIC. The SIO has responsibility for "leading and managing the FDIC-wide comprehensive, all-hazards intelligence support program and its functions." The SIO also has responsibilities including "planning, organizing, and implementing intelligence support activities in order to support mission critical objectives and aid in the evaluations of contingency operations." Given the critical nature of the SIO responsibilities to the mission of the FDIC, the former Deputy to the Chairman and Chief Operating Officer designated the SIO as one of the FDIC's more than 800 "essential" personnel for the purposes of the global pandemic caused by COVID-19.[88]

However, the FDIC neither established an alternate (backup) for the SIO nor cross-trained other staff on the SIO's duties and responsibilities. As a result, the FDIC did not have other personnel who could perform the SIO duties. This gap in contingency planning had a practical effect. When the SIO was unavailable (vacation or leave), threat-related briefings and communications to FDIC stakeholders did not occur. For example, the SIO notified FDIC stakeholders that they would not receive the SIO regular Global Intelligence Update during a week when the SIO was out of the office. In addition, on April 12, 2021, the SIO began working on a detail assignment. There has been no replacement named to fill this position since that time.

In addition, the FDIC had not developed a succession plan to mitigate the risk of a prolonged absence or departure of the SIO. The SIO position requires specialized

[88] Notification to the SIO, entitled *Emergency Authorization Letter for Essential Personnel* (May 2020), from the former Deputy to the Chairman and Chief Operating Officer. According to this notification, essential personnel have responsibility for performing critical business activities needed to minimize disruption to FDIC operations during challenging conditions.

knowledge, skills, and abilities to research, interpret, analyze, and disseminate classified and unclassified information. The SIO position also requires a TS/SCI clearance, and knowledge of both the Financial Services Sector and FDIC business functions and programs. Finding and hiring a successor who possesses such capabilities could take a prolonged period of time. A succession plan would help to ensure the continued, uninterrupted sharing of threat information with officials administering FDIC programs and operations, should the SIO depart the FDIC. The lack of contingency and succession planning for the SIO occurred because the FDIC had not defined contingency and succession plans as recommended by GAO Internal Control Standards.

Further, we found that the Intelligence Support Program's records storage practices exacerbated the risk associated with an unexpected absence or departure of the SIO. Unclassified threat information was stored in the SIO's personal FDIC email folders and network drives, rather than in a centralized system. As a result, that unclassified threat information would not be readily accessible to other FDIC personnel if the SIO unexpectedly departed the FDIC.

Storing unclassified threat information on a centralized platform would allow the SIO to more efficiently and effectively share relevant threat information with FDIC stakeholders who need it. For example, storing the SIO's research on the SolarWinds, Inc. (SolarWinds) compromise[89] in a centralized system would allow supervisory personnel in the FDIC (including the RMS Operational Risk group, security professionals in the OCISO, and risk managers in ORMIC) to readily access the information. The FDIC established a shared electronic storage site in September 2020 after we identified this exception. The site is available to ITCIP and other DOA personnel.

The availability of relevant and actionable threat information is critical to supporting informed supervisory decision-making. The lack of contingency and succession planning for the SIO, together with sound records storage practices, presented a risk to the timely flow of all hazard threat information in support of FDIC operations and programs. This risk could become more significant if the SIO became unavailable during a national emergency.

[89] In December 2020, the National Security Council established a task force known as the Cyber Unified Coordination Group (UCG) to coordinate the investigation and remediation of the significant cyber incident involving SolarWinds. The UCG determined that an Advanced Persistent Threat (APT) actor compromised the software supply chain of SolarWinds and inserted malicious code into certain updates of the SolarWinds Orion software product. Once customers of SolarWinds applied these Orion software updates, the APT actor gained unauthorized access to the customers' network environments.

Recommendations

We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

17. Establish a backup for the SIO to ensure the continued implementation of key duties and responsibilities.

18. Establish a succession plan to addresses a potential departure of the SIO.

19. Require that the SIO maintain unclassified threat information on a centralized storage platform so that it would be accessible by other FDIC personnel with a business need.

Expanded Training Needed for the SIO

GAO Internal Control Standards identify employee training as a key element in the success of an organization's operations. According to the Internal Control Standards, training focuses on developing and retaining the knowledge, skills, and abilities that enable employees to develop appropriate competencies for their roles. Training can be accomplished through a variety of venues, such as classroom training, e-learning, and professional conferences. According to the GAO, training assists Federal agencies in achieving their missions and goals by improving individual and, ultimately, organizational performance.

The SIO has responsibility for "leading and managing the FDIC-wide comprehensive, all-hazards intelligence support program and its functions. The intelligence support program provides executives and senior staff with accurate and timely all-source intelligence with the potential to impact the FDIC and the U.S. financial sector." The SIO also has responsibility for "interacting with various senior FDIC officials in providing focused intelligence designed to support their specific mission" and maintaining "knowledge of the mission, functions, and organizational structure of FDIC."

However, our review of the SIO's training records for the years 2015 through 2020 found that although the SIO had taken training on intelligence sharing and threats in the Financial Services Sector, the SIO had taken only two courses on FDIC banking

mission areas and business operations[90], and these courses were completed more than 6 years ago in 2015.[91] The FDIC did not establish minimum training requirements for the SIO position and therefore, the SIO did not take, additional training in FDIC mission areas and business operations.

Adequate knowledge of FDIC's mission areas and business operations is critical to the SIO's ability to provide "focused intelligence" to FDIC officials as described in the SIO's Position Description. Expanded training in the FDIC's mission areas and business operations would facilitate the SIO's efforts to determine the types of threat information that FDIC officials need to support their programs, operations, and business decisions. Expanded training could also identify new ways in which to effectively integrate information into the FDIC policy development and decision-making activities.

Recommendation

We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

20. Establish minimum training requirements for the SIO consistent with the SIO's responsibilities.

Processing of Security Clearances Needs Improvement

As previously stated, the Position Description for the Regional Directors requires a TS/SCI clearance. The FDIC, however, did not take action to obtain required security clearances for two of the six Regional Directors until we identified these exceptions in May 2020.

One Regional Director had been in this role for almost 2-1/2 years when we identified that he did not have a security clearance at the TS/SCI level (since January 2018).[92] That Regional Director had a security clearance at only the Secret level. The other Regional Director had been in this role for 9 months when we identified the exception (since September 2019).[93] This Regional Director had no security clearance.

[90] The FDIC's mission areas and operations include, for example, bank supervision and regulation, complex institution supervision and resolution, receivership operations, financial operations, information technology and cybersecurity, and acquisition and procurement.
[91] These courses were the *One FDIC: A Program About Our Corporate Culture* completed in October 2015 and the *Examination School for Non-Examiners* completed in December 2015.
[92] The FDIC appointed the individual to serve as this Regional Director in January 2018.
[93] The FDIC appointed this individual to serve as a Regional Director in September 2019.

According to SEPS:

- In the case of one Regional Director, a representative of SEPS stated that a completed FDIC Form 1600/13 or other written request from RMS to initiate the security clearance could not be located. However, the SEPS representative stated that SEPS likely received such a request because SEPS initiated a background investigation for a TS clearance for the Regional Director in December 2017. The SEPS representative added that the contractor responsible for processing the security clearance no longer worked for the FDIC, and no additional information about the request was available. In July 2019, SEPS completed and adjudicated the TS background investigation. However, due to another mistake, SEPS did not issue a TS clearance for the Regional Director. A SEPS representative attributed the oversight to inadequate monitoring by SEPS personnel of the contractor responsible for processing security clearances. In addition, SEPS did not request SCI access for the Regional Director.

- Regarding the other Regional Director, SEPS determined that the RMS Administrative Officer in the Regional Office did not submit an FDIC Form 1600/13 for a TS/SCI security clearance to SEPS concurrent with the Regional Director's appointment. Because the individual serving as the Regional Director was not required to have a security clearance in the position held prior to the appointment as Regional Director, the individual did not hold a security clearance when starting as Regional Director. This Regional Director serves as the successor to the RMS Director in the event of a devolution of the FDIC. It is, therefore, critical that this Regional Director hold a security clearance because this individual may be required to serve in place of the RMS Director during a devolution.

On July 6, 2020, after we had informed RMS and SEPS of these two exceptions, RMS provided SEPS with two requests to process TS/SCI clearances for both Regional Directors.[94] On July 23, 2020, SEPS issued a TS clearance for one Regional Director. On March 8, 2021, SEPS issued a TS clearance for the other Regional Director. As of July 15, 2021, SEPS had not yet received approval for SCI access for either Regional Director.[95]

[94] RMS submitted both requests on FDIC Form 1600/13, *Personnel Security Action Request*. Divisions and Offices must provide SEPS with a completed FDIC Form 1600/13 whenever an employee begins working in a position that requires a security clearance.

[95] [redacted]

If the FDIC does not take timely action to obtain security clearances for the Regional Directors consistent with their Position Description, the Regional Directors are not able to access information needed to fulfill their duties. According to written justifications completed by RMS, such duties include participating in classified briefings with FDIC personnel and outside agencies such as the FBIIC, and making supervisory decisions regarding resource allocations and the risk-focusing of examinations and supervisory-related activity.

Recommendations

We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

21. Implement measures to ensure that SEPS processes requests for security clearances submitted by Divisions and Offices in a timely manner.

22. Implement measures to ensure that Administrative Officers promptly inform SEPS when employees enter into new positions that require a security clearance.

Unclassified Threat Information Not Categorized for Security Purposes

NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), requires Federal agencies to categorize their unclassified information as high, moderate, or low.[96] These three security categories reflect the potential impact on the agency should there be a loss of confidentiality, integrity, or availability of the information. Agencies use the security categories in NIST FIPS 199 to determine the proper security controls needed to protect unclassified information and the systems that process the information.

According to NIST FIPS 199, agencies must categorize their information based on the information's type. NIST FIPS 199 defines an information type as a specific category of information, such as privacy, medical, proprietary, financial, investigative, contractor sensitive, or security management. NIST SP 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008), provides guidance to assist agencies in identifying and categorizing

[96] NIST FIPS publications are mandatory under FISMA. However, the FDIC has taken the position that NIST FIPS publications are not binding on the FDIC because the Secretary of Commerce, who approves FIPS publications, does not have the authority to impose mandatory requirements on the FDIC. Nevertheless, the FDIC views NIST FIPS publications as guidance for "best practices" in implementing security measures for information and information systems.

their information types. NIST SP 800-60 states that agencies shall identify all applicable information types and create a catalog describing each information type and its associated security category. The FDIC's Chief Information Security Officer (CISO), who reports to the Chief Information Officer (CIO), coordinates the FDIC's implementation of NIST security standards and guidelines, including FIPS 199 and SP 800-60.

In response to guidance in NIST SP 800-60 to create a catalog of data types, the FDIC created a Conceptual Data Model (CDM) containing 261 information types. Each information type in the CDM includes a security category for the information type's confidentiality, integrity, and availability. However, none of the 261 information types in the CDM addressed the unclassified threat information collected, stored, disseminated by the SIO.

The SIO labeled threat information disseminated throughout the FDIC with a variety of markings to help ensure recipients safeguarded the information from unauthorized disclosure.[97] However, the FDIC had not categorized the threat information managed by the SIO as high, moderate, or low, because the FDIC had not implemented an effective process for updating the CDM when Divisions and Offices begin using new information types. The SIO began sharing unclassified threat information after the FDIC established the SIO position in April 2015. However, the FDIC had not updated the CDM since September 2013. As a result, the CDM did not contain an information type that addressed the threat information managed and shared by the SIO.

According to NIST SP 800-60, assigning proper security categorizations to information types is a critical step in implementing the NIST Risk Management Framework (RMF).[98] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016), requires Federal agencies to use the NIST RMF to manage the security and privacy risks associated with their information and information systems.[99] Agencies use the RMF to guide and inform the categorization of information and information systems; the selection, implementation, and assessment

[97] Such markings included, but were not limited to, Sensitive But Unclassified (SBU), No Foreign Nationals (NOFORN), Releasable by Information Disclosure Official (RELIDO), Releasable to USA and Five Eyes (REL TO USA, FEVY), and For Official Use Only (FOUO). In addition, the SIO marked the Global Intelligence Updates for restricted distribution due to the sensitivity of the sources used by the SIO to develop the updates.
[98] NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (December 2018), defines the RMF as a life cycle process for protecting information systems.
[99] The FDIC determined that OMB Circular A-130 is "generally applicable" to the FDIC, to the extent that the Circular aligns with OMB's statutory authorities, does not impose obligations on the FDIC based on statutes that are legally inapplicable to the FDIC, and does not conflict with the FDIC's independence, statutory obligations, or regulatory authority. FDIC Review of OMB Circular A-130 (July 28, 2016).

of security and privacy controls; and the continuous monitoring of security and privacy controls. Without an effective process for identifying new information types and including them in the CDM, the FDIC cannot be sure that new information types will be subject to the RMF. As a result, the FDIC may not categorize sensitive information or implement proper controls to ensure the confidentiality, integrity, or availability of the information.

Recommendations

We recommend that the CIO:

23. Establish a process to ensure that the CDM maintains current information regarding the information types used by the FDIC.

We recommend that the CISO:

24. Categorize the unclassified threat information managed by the SIO and include this information in the CDM.

25. Ensure that appropriate security controls are implemented to protect unclassified threat information by the SIO consistent with NIST guidance.

FDIC COMMENTS AND OIG EVALUATION

On November 5, 2021, FDIC Management provided a written response to a draft of this report. The FDIC response is presented in its entirety in Appendix 5. In its response, FDIC Management stated that the OIG's recommended control enhancements have merit. For example, FDIC Management stated that the agency will build a community of practice for analysis and dissemination of threat information across the FDIC. FDIC Management also stated that in October 2021, it established a new Intelligence and Threat Sharing Group, and this Group will report to a newly established Chief of Staff to the Chief Operating Officer. The FDIC believes that centralizing and elevating these functions will help to enhance focus and coordination among intelligence sharing, counterintelligence, and insider threat responsibilities. FDIC Management further stated that the agency can improve documentation regarding its existing processes and procedures for sharing threat information.

In its response, FDIC Management concurred with 22 of the 25 recommendations in this report. It partially concurred with two additional recommendations (Recommendations 12 and 18). FDIC Management proposed corrective actions that were sufficient to address 24 recommendations. Therefore, we consider them to be resolved.

FDIC Management, however, did not concur with Recommendation 14: To establish a means for Regional Offices to handle classified information once it is shared, including the infrastructure to securely handle, transmit, discuss, store, and dispose of classified information. FDIC Management stated that the construction of SCIFs and other associated infrastructure in the FDIC's Regional Offices would not be justified given the significant costs required to establish and maintain the facilities. Our recommendation does not suggest that the FDIC should construct SCIFs for each of the Regional Offices. As discussed in this report, there are three classified information levels: confidential, secret, and top secret (TS). In addition, there is a category of classified information commonly associated with the TS level, known as Sensitive Compartmented Information (SCI). Any information classified below the TS/SCI level does not need to be shared or maintained within a SCIF, and therefore would not require the construction of a SCIF. The FDIC has certified justifications annually for TS/SCI clearances. In these justifications, RMS has stated that the Regional Directors need access to classified information to carry out their supervisory responsibilities. As a result, when the FDIC shares classified information with the Regional Directors, they will need a means to securely handle, transmit, discuss, store, and dispose of the information. Coordination with other agencies may be part of the solution; however, that will not address how classified information in

the possession of the Regional Directors will be handled. Therefore, we consider Recommendation 14 to be unresolved. We will work with FDIC management to attempt to reach resolution of this recommendation during the audit follow-up process.

Following issuance of a draft of this report, the FDIC provided documentation to demonstrate that it had taken corrective actions to address three recommendations. For one recommendation (Recommendation 19), we completed our review of the documentation provided and confirmed that the corrective actions were responsive, thus our recommendation will be closed. For the remaining two recommendations (Recommendations 21 and 22), the documented corrective actions will take time to review. We plan to complete our review of the submitted materials following issuance of the report. Accordingly, these two recommendations are considered resolved but will remain open at the time of issuance of this report.

All other recommendations in this report will also remain open until we confirm that corrective actions have been completed by the FDIC and that the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 6.

.

Objective

The audit objective was to determine whether the FDIC established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions.

We conducted this performance audit from May 2019 through July 2021 in accordance with generally accepted government auditing standards (2011 version).[100] These 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.

Scope and Methodology

The scope of the audit focused on the FDIC's internal processes for sharing threat information among supervisory personnel in the Headquarters and Regional Offices. The audit did not assess the FDIC's examination procedures designed to identify and assess threats at FDIC-supervised financial institutions or to ensure that financial institutions obtain and use threat information to protect their operations. We plan to initiate a separate review that will assess the effectiveness of the FDIC's supervisory approach for ensuring FDIC-supervised financial institutions receive and use threat information to protect their operations.

For purposes of the audit, we used the DHS definition of the term "threat." DHS defines threat as "a natural or human-created occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property."[101] The scope of the audit was limited to threats of an operational nature. Such threats can be man-made or natural, and involve circumstances or events originating external to an insured financial institution that have the potential to adversely impact its operations and threaten its safety and soundness. Examples include cyber attacks, money laundering, terrorist financing, pandemics, and natural disasters such as hurricanes, tornadoes, and floods. The scope of the audit did not include insider threats, which DHS defines as the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States.

[100] In July 2018, the Comptroller General of the United States issued a revision to the generally accepted government auditing standards which became effective for performance audits beginning on or after July 1, 2019. Because we initiated this audit in May 2019, we followed the 2011 standards.
[101] See DHS *Risk Lexicon Terms and Definitions, 2017 Edition – Revision 2* (October 2017).

To obtain an understanding of threat information sharing concepts and principles, we reviewed relevant Federal and private-sector plans, guidance, and reports, including:

- DHS *Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community* (October 2016);
- *The National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*;
- *The Financial Services Sector-Specific Plan 2015*;
- The White House *National Strategy for Information Sharing and Safeguarding* (December 2012);
- NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing* (October 2016);
- GAO report, entitled *CYBERSECURITY: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information* (Report No. GAO-15-509, July 2015); and
- The Office of the Inspector General of the Intelligence Community *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (Report No. AUD-2019-005-U, December 2019).

We also spoke with representatives of the Treasury Department's Office of Critical Infrastructure Protection and Compliance Policy, DHS' Cybersecurity and Infrastructure Security Agency, and DHS' Office of Intelligence and Analysis to obtain an understanding of Government-wide practices and challenges associated with sharing operational threat information. In addition, we spoke with representatives of the Federal Reserve Board, OCC, NCUA, and other state regulators to discuss the processes those regulators employ and the challenges they face with respect to acquiring, analyzing, disseminating, and using threat information to guide bank supervisory activities.

Based on our review of relevant Federal and private-sector plans, guidance, and practices (including those specifically referenced above), and practices employed by other Federal agencies and industry organizations, we developed a Threat Sharing Framework consisting of four life-cycle components: (1) acquiring relevant and actionable threat information from internal and external sources; (2) analyzing threat information to determine how it can support FDIC programs, operations, and

decision-making; (3) disseminating threat information to stakeholders who need it; and (4) obtaining feedback from stakeholders regarding the utility of threat information and how threat information sharing processes can be improved. Based on our review of standards, guidance, and practices published the GAO, OMB, PMI, and others, we included elements of Governance and Management in the Threat Sharing Framework.[102] We used the Threat Sharing Framework to guide our audit work and summarize our results.

We used the GAO *Standards for Internal Control in the Federal Government* (Internal Control Standards) (September 2014) as the primary criteria for assessing the effectiveness of FDIC's threat information sharing processes. The Internal Control Standards define 17 specific principles that are necessary to establish an effective internal control system at Federal agencies. Our audit assessed certain attributes pertaining to 8 of these 17 principles. The report findings present the internal control deficiencies we identified pertaining these eight principles. Because we limited the scope of our work to 8 of the 17 principles, the audit may not have identified all internal control deficiencies existing at the time of our work.

We supplemented the Internal Control Standards with the following additional criteria:

- FDIC policies, procedures, and guidance, including:
    - Directive 1360.9, *Protecting Sensitive Information* (April 2007);
    - Directive 1210.01, *Records and Information Management Program* (March 2021);
    - Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (October 2018);
    - Enterprise Risk Management Standard Operating Procedure (May 2021);
    - RMS *Regional Cyber Incident Response Guide (February 2021);*
    - Circular 1600.3, *National Security Program* ((issued in September 2001 and updated in December 2017); and
    - Directive 2120.1, *Personnel Security and Suitability Program for Applicants and Employees* (January 2020).

[102] Such standards, guidance, and practices included GAO's Internal Control Standards, OMB Memorandum M-18-19*, Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA)* (June 2018); OMB Circular A-11, *Preparation, Submission, and Execution of the Budget* (August 2021); PMI's *The Standard for Program Management* (Fourth Edition, 2017); and other industry publications on program and project management.

- NIST security standards and guidance, including:
    - Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004); and
    - Special Publication 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008).

- Government-wide policy, including:
    - Presidential Executive Order No. 12968, *Access to Classified Information* (August 1995);
    - Presidential Executive Order No. 13526, *Classified National Security Information* (December 2009);
    - OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016); and
    - OMB Memorandum M-18-19, Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA) (June 2018);

- Industry publications on program and project management, most notably the Project Management Institute's *The Standard for Program Management* (Fourth Edition, 2017).

To assess the FDIC threat information sharing practices, we interviewed the following individuals:

- RMS personnel in Headquarters, including the RMS Director, RMS Deputy Director for Operational Risk, and supervisory staff in the IT Supervision Branch, AML and Cyber Fraud Branch, and Critical Infrastructure Resilience Team;

- All six Regional Directors and selected members of their staff who had responsibility for overseeing examination strategies and activities related to BSA/AML, IT, and other operational risks;

- Officials in the DOA Corporate Services Branch, including the SIO and SEPS personnel responsible for processing security clearances;

- Officials in CISR, including the Acting Senior Deputy Director for Supervision and Resolution and the Deputy Director, Risk Assessment Branch; and

- Other FDIC officials, including the CFO, CRO, DRR Director and DRR staff, and DIR staff.

We also reviewed selected classified briefing materials in the FDIC's SCIF. Further, we reviewed unclassified threat information, such as RMS' weekly *Cybersecurity Brief*, bi-weekly *RMS Cybersecurity and Critical Infrastructure Protection Update*, *Quarterly Operational Risk Book*, ad hoc *Advisory Bulletins* covering various threats, a webinar with examiners on the SolarWinds compromise, and other written communications shared by the RMS Operational Risk group with supervisory staff in the Regional and Field Offices. We reviewed the materials to gain an understanding of the type of threat information the FDIC acquires, analyzes, and disseminates.

We did not rely on computer processed information to accomplish our audit objective. We determined that information system controls were not significant to the audit objective and, therefore, we did not evaluate the overall effectiveness of information system controls. We corroborated information to support our audit conclusions with information from various sources, including supporting documentation, and testimonial evidence from subject matter experts. In addition, we assessed the risk of fraud and abuse related to our objective in the course of evaluating audit evidence.

Appendix 2 Acronyms and Abbreviations

AML	Anti-Money Laundering
BSA/AML	Bank Secrecy Act/Anti-Money Laundering
CCIWG	Cybersecurity and Critical Infrastructure Working Group
CDM	Conceptual Data Model
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
CIOO	Chief Information Officer Organization
CIRP	Cyber Incident Response Plan
CISR	Division of Complex Institution Supervision and Resolution
COO	Chief Operating Officer
CRO	Chief Risk Officer
CSBS	Conference of State Bank Supervisors
DHS	Department of Homeland Security
DHS Framework	DHS Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community
DIR	Division of Insurance and Research
DOA	Division of Administration
DOF	Division of Finance
DRR	Division of Resolutions and Receiverships
EO	Executive Order
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FDI	Federal Deposit Insurance (FDI) Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
FMFIA	Federal Managers' Financial Integrity Act
FOUO	For Official Use Only
FRB	Federal Reserve Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSIC	Federal Senior Intelligence Coordinator
FSOC	Financial Stability Oversight Council
FSSCC	Financial Services Sector Coordinating Council
GAO	Government Accountability Office
Interagency Guidelines	Interagency Guidelines Establishing Information Security Standards
InTREX	IT Risk Examination Program
IT	Information Technology
LCFI	Large and Complex Financial Institutions
LIDI	Large Insured Depository Institutions
NCUA	National Credit Union Association
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
OIG	Office of the Inspector General

ORMIC	Office of Risk Management and Internal Controls
PPD	Presidential Policy Directive
RMF	NIST Risk Management Framework
RMS	Division of Risk Management Supervision
RRS	Record Retention Schedule
SAR	Suspicious Activity Report
SCIF	Sensitive Compartmented Information Facility
SEPS	Security and Emergency Preparedness Section
SIO	Senior Intelligence Officer
SOP	Standard Operating Procedure
SP	Special Publication
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
Treasury Department	Department of the Treasury
TS/SCI	Top Secret security clearance with Sensitive Compartmented Information
ViSION	Virtual Supervisory Information on the Net

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

Date: April 30, 2020

Memorandum To: Doreen R. Eberley
Director, Division of Risk Management Supervision

Ricardo R. Delfin
Director, Division of Complex Institution Supervision and Resolution

Maureen E. Sweeney
Director, Division of Resolutions and Receiverships

Mark Pearce
Director, Division of Depositor and Consumer Protection

Mark F. Mulholland

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

Subject **Management Advisory Memorandum** | *Cybersecurity Incident Reporting by Insured Financial Institutions* | No. 2019-003

While conducting our ongoing audit on receiving and sharing threat information, we identified a concern warranting the attention of the FDIC. Specifically, Federal regulations applicable to insured financial institutions do not address the reporting of cyber incidents to Federal bank regulators unless the incidents involve the compromise of customer information. Other types of cyber incidents that can threaten an institution's safety and soundness are not required to be reported to Federal bank regulators. Such incidents include destructive[1] cyber attacks that can render an institution's information systems inoperable, impair an institution's ability to conduct business, and potentially cause an institution to fail. Reporting such incidents would provide the FDIC with critical information that could enhance the effectiveness of its supervisory activities and resolution planning efforts.

Background

Insured financial institutions rely heavily on information technology (IT) to facilitate transactions with customers, creditors, and other institutions. While IT offers significant advantages, it also introduces the risk of cyber incidents that can disrupt critical banking operations, inflict financial harm on individuals, and cause a loss of confidence among institution customers. The *Joint*

[1] We use the term "destructive" in this memorandum because the Federal Financial Institutions Examination Council (FFIEC) uses the term in its Joint Statements, such as the *Joint Statement, Destructive Malware* (March 2015), and in the *Business Continuity Management* booklet, which is a component of the *FFIEC Information Technology Examination Handbook*.

Privileged and Sensitive Information | For Official Use Only

Statement on Heightened Cybersecurity Risk (January 2020) issued by the FDIC and the Office of the Comptroller of the Currency (OCC) states that disruptive and destructive cyber attacks against financial institutions have increased in frequency and severity in recent years. According to this joint statement, cyber actors often use malicious software known as malware to exploit weaknesses in information systems at financial institutions. The *Joint Statement on Heightened Cybersecurity* states:

> *Destructive malware introduced into a financial institution's systems has the potential to alter, delete, or otherwise render production data and systems unusable. Depending on the scope of the attack, the type of backup processes used, and other controls employed, the financial institution's data and system backups may also be similarly affected by a destructive malware attack, severely affecting the financial institution's ability to recover operations.*[2]

Ransomware is a particular type of destructive malware that cyber criminals have used to extort money from U.S. businesses. According to the Department of Homeland Security (DHS), "ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks, locking up private sector organizations and government agencies alike."[3] The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3)[4] reported that in 2019, it received 2,047 complaints of ransomware with adjusted losses of over $8.9 million.[5] We have identified this risk area as part of the Top Challenges facing the FDIC.[6]

Cyber criminals can introduce ransomware into a financial institution's IT network in a variety of ways. For example, a cyber criminal may send a fraudulent email to employees of an institution that contains an attachment with malware or a link to a compromised Web site. If an employee clicks on the attachment or visits the compromised Web site, the ransomware may be downloaded onto the employee's computer and thus the institution's systems. This malware may render the institution's systems and data unusable by encrypting the systems and data, until a "ransom" is paid. The institution may pay a ransom, typically in the form of virtual currency, in exchange for a decryption key that will unlock the institution's systems or data. Even with preventive controls in place, financial institutions may fall victim to destructive malware attacks such as ransomware.

The interconnected nature of financial services elevates the potential impact that cyber incidents can have on financial institutions. Insured financial institutions can have business relationships with, or provide banking services to, other financial institutions. In addition, many insured financial institutions rely on third-party service providers to provide critical services, such as loan processing; deposit processing; and the origination, processing, and settlement of payments and financial transactions. Therefore, a cyber incident at one financial institution or service provider could impact other entities in the financial services sector. If the associated impact is

---

[2] See the FDIC's and OCC's *Joint Statement on Heightened Cybersecurity Risk* (January 2020).
[3] See DHS' *CISA Insights, Ransomware Outbreak* (August 2019).
[4] The FBI's IC3 provides the public with a mechanism for reporting information concerning suspected Internet-facilitated criminal activity.
[5] See IC3's *2019 Internet Crime Report*. According to this Report, the adjusted losses figure "does not include estimates of lost business, time, wages, files, or equipment, or any third party remediation services acquired by a victim. . . .the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents."
[6] See *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (February 2020).

wide-spread, the cyber incident could result in a loss of confidence among a broad set of customers and threaten the stability of financial institutions.

A recent cyber incident at Finastra, a company that provides financial technology services to banks and other financial institutions around the globe, illustrates the risk associated with interconnected financial services. In March 2020, Finastra publicly disclosed that it had been the victim of what appeared to be a ransomware attack which caused the firm to take its servers off-line for a period of time.

The Need for Timely Cyber Incident Information

Each Regional Office within the FDIC has developed an internal *Cyber Incident Reporting and Response Guide*. These guides are intended to help ensure that Regional Offices handle cyber incidents reported by financial institutions and their service providers in a consistent manner. The *Cyber Incident Reporting and Response Guides* state that "[k]nowing about and responding to incidents at FDIC-supervised entities[7] is important to the FDIC mission."

The *Cyber Incident Reporting and Response Guides* identify several reasons why the FDIC would benefit from receiving information about cyber incidents. The Guides state that the FDIC can better tailor the scope of examinations if the FDIC knows about financial institutions' cyber incidents. In addition, the FDIC can provide advice to institutions affected by cyber incidents based on the FDIC's experience in supervising other entities. Further, the *Cyber Incident Reporting and Response Guides* state that receiving cyber incident information allows the FDIC to conduct analysis across entities to improve supervisory guidance; form effective, industry-wide supervisory programs; and provide information to other institutions to help them protect against similar incidents.

The *Cyber Incident Reporting and Response Guides* also recognize that a cyber incident may so severely impact an institution's safety and soundness that it ultimately causes the institution to fail. The Guides state that the sooner the FDIC knows of such incidents, the better it can prepare for the institution's failure. Cyber incidents can disrupt information systems and compromise data in a matter of minutes. The potential severity and swiftness of a cyber incident could compress ordinary resolution planning timelines. Therefore, prompt reporting of destructive cyber incidents by financial institutions would facilitate resolution planning activities.

Regulations Do Not Address Reporting for Destructive Cyber Incidents Threatening the Safety and Soundness of Institutions

The Federal bank regulators have promulgated *Interagency Guidelines Establishing Information Security Standards* (Interagency Guidelines) and published them in the Code of Federal Regulations (CFR).[8] The Interagency Guidelines establish standards for developing and implementing safeguards to protect the security, confidentiality, and integrity of customer

[7] The *Cyber Incident Reporting and Response Guides* define the term "entity" as a financial institution or its service provider.
[8] The Federal bank regulators consist of the FDIC, OCC, Board of Governors of the Federal Reserve System (FRB), and former Office of Thrift Supervision (OTS). The FDIC published the Interagency Guidelines for the entities subject to its jurisdiction in 12 CFR Part 364, App. B and 12 CFR Part 391, subpart B, App. B.

information. The Interagency Guidelines, and supplemental guidance published in the CFR by the Federal bank regulators,[9] state that every financial institution should develop and implement a Response Program "to address incidents of unauthorized access to customer information in customer information systems."[10] According to the Interagency Guidelines and supplemental guidance, an institution's Response Program should include procedures for "notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information." This reporting responsibility also applies when an incident occurs at an institution's service provider.

However, the Interagency Guidelines and supplemental guidance only apply to incidents that compromise customer information. Federal regulations do not address reporting to Federal bank regulators for other types of destructive cyber incidents that could jeopardize the safety and soundness of an institution. Such incidents include, for example, denial of service attacks and ransomware attacks that can disrupt an institution's operations and inflict severe and potentially irreversible damage to information systems and data.

The FFIEC encourages financial institutions that are victims of cyber attacks involving extortion to notify their primary regulator.[11] [redacted]

While risk management examinations and SARs can provide valuable information about cyber attacks, they are not designed to ensure prompt and timely notification to the FDIC about cyber incidents affecting the safety and soundness of insured institutions.[12]

Cyber Incident Reporting Requirements by State Regulators

In recent years, certain state regulators have established requirements for state-chartered banks to promptly report destructive cyber incidents. For example, the Finance Commission of Texas issued a rule that became effective on January 2, 2020, that requires state-chartered banks to promptly notify the Banking Commissioner of material cybersecurity incidents.[13] Cybersecurity incidents covered by the rule include, but are not limited to, incidents that "adversely impact, at least temporarily, the ability of the bank to effect transactions on behalf of customers, accurately report transactions to customers, or otherwise conduct bank business." The Texas rule requires state-chartered banks to notify the Banking Commissioner as soon as

[9] See *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, Part 364, App. B (Supp. A). The FDIC, OCC, FRB, and former OTS issued this supplemental guidance to interpret the requirements of section 501(b) of the Gramm-Leach-Bliley Act and the Interagency Guidelines.
[10] 12 CFR Part 364 defines customer information as any record containing non-public personal information about a customer that is maintained by or on behalf of the institution.
[11] See FFIEC *Joint Statement, Cyber Attacks Involving Extortion* (November 2015).
[12] Institutions are required to file a SAR within 30 calendar days following initial detection of facts triggering the SAR filing requirement. The SAR filing deadline may be extended an additional 30 days (up to a total of 60 calendar days) if no suspect is identified.
[13] See 7 TAC §3.24; 44 TexReg 3381 (Jan. 2, 2020).

practicable, prior to customer notification, but not later than 15 days following the entity's determination that a qualifying cybersecurity incident has occurred.

In addition, the New York State Department of Financial Services promulgated a regulation which became effective on March 1, 2017, that requires state-chartered banks to promptly report cybersecurity events that have "a reasonable likelihood of materially harming any material part of the normal operation(s)" of an institution.[14] According to this regulation, entities must notify the Superintendent of Financial Services "as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred that" meets the criteria in the regulation.

Conclusion

Establishing a Federal requirement for the prompt reporting of destructive cyber incidents could provide the FDIC and other Federal bank regulators more consistent information to assess threats and implement supervisory actions in a timely manner. Such information could also assist the FDIC in its role as receiver for failed financial institutions, as it would allow for timely preparations for a potential resolution.

We request that you provide a written response to this Memorandum describing the actions the FDIC plans to take to address the concern described above regarding institutions not being required to promptly report destructive cyber incidents. The response should describe the timeframes for taking those actions. Please submit your response by May 21, 2020.

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

cc: Martin D. Henning, RMS
John F. Vogel, RMS
Titus S. Simmons, RMS
Krista Hughes, CISR
David J. Tedesco, DRR
Lorraine D. Rushing, DCP
Nicholas Podsiadly, General Counsel
Brandon Milhorn, Deputy to the Chairman and Chief of Staff
Arthur J. Murton, Deputy to the Chairman for Financial Stability
E. Marshall Gentry, DOF

[14] See Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500, (March 1, 2017).

FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990 Division of Risk Management Supervision

May 21, 2020

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

FROM: Doreen R. Eberley
Director, Division of Risk Management Supervision

SUBJECT: Management Advisory Memorandum | Cybersecurity Incident Reporting by Insured Financial Institutions | No. 2019-003

Thank you for your April 30, 2020 advisory memorandum regarding cybersecurity incident reporting. I am responding on behalf of the other division directors to whom you addressed the advisory memorandum, as oversight of financial institutions' information technology systems is the responsibility of the Division of Risk Management Supervision. As we have discussed, the possibility of promulgating a new, national cybersecurity incident reporting regulation is something the federal banking regulators have considered.

We have reinitiated internal and external conversations on this topic. In these early conversations, we are discussing the purpose of collecting this information and the thresholds for collection needed to support those purposes. We have also discussed collection mechanisms. Finally, we have discussed the cost to the industry relative to the potential benefit to be derived.

The next step is to gather an interagency team to draft a rule for notice and comment. The timeframe for this analysis will depend on the resource quantity assigned to this initiative by each agency, and the speed with which they can reach agreement. We believe that September 30, 2020 is a reasonable timeframe goal for publishing a draft rule for notice and comment.

We appreciate the review of this area and your advice, and as outlined above we are taking actions relative to this topic. If you have questions regarding this response please contact Martin Henning, whose team will be facilitating the FDIC portion of this effort.

cc: Ricardo R. Delfin, Director, Division of Complex Institution Supervision and Resolution
Maureen E. Sweeney, Director, Division of Resolutions and Receiverships
Mark Pearce, Director, Division of Depositor and Consumer Protection

Office of Inspector General

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

Date: January 22, 2021

Memorandum To: Doreen R. Eberley
Director, Division of Risk Management Supervision

Mark F. Mulholland

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

Subject: **Management Advisory Memorandum** | Potential Exposure of Insured Financial Institutions to the SolarWinds Compromise | No. 2021-001

In December 2020, the National Security Council established a task force known as the Cyber Unified Coordination Group (UCG)[1] to coordinate the investigation and remediation of the significant cyber incident involving SolarWinds, Inc. (SolarWinds).[2] The UCG determined that an Advanced Persistent Threat (APT) actor compromised the software supply chain of SolarWinds and inserted malicious code into certain updates of the SolarWinds Orion software product. Once customers of SolarWinds applied these Orion software updates, the APT actor gained unauthorized access to the customers' network environments. The UCG noted that there are approximately 18,000 public and private sector customers of the Orion software product.

On December 17, 2020, while conducting research related to the SolarWinds compromise, we identified information pertaining to FDIC-insured financial institutions on two publicly-available websites.[3] The information included a decoded version of SolarWinds software that identified domain names (web sites) of entities possibly exposed to the compromise. The information specifically identifies at least 11 financial institutions, including institutions that are insured by the FDIC. We did not assess the accuracy or completeness of this information.

We immediately provided the information to the Deputy Director, Division of Risk Management Supervision (RMS), Operations Branch, and notified the FDIC's Senior Intelligence Officer, and the Chief Information Security Officer. We took these actions so that FDIC officials could assess the information to determine whether it could be used to inform supervisory strategies in

[1] See the Joint Statement issued by the Federal Bureau of Investigation, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence, and the National Security Agency (January 2021) at https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.
[2] SolarWinds, Inc. is a software development company that offers products and services to assist entities in managing their networks, systems, and information technology infrastructure.
[3] See https://twitter.com/Bank_Security/status/1339473635078225920 and https://github.com/5u3e10px/Suburst-DGA-Domains-Decoded.

Privileged and Sensitive Information | For Official Use Only

response to the SolarWinds compromise. Based upon an assessment of the information, the FDIC could, for example, decide to share the information with regional or field office examination staff; confer with other Federal or state bank regulatory agencies; notify affected financial institutions; or take other potential actions. We request that you notify us if the FDIC takes any actions in response to the information provided.

If you would like to discuss the issues identified in this Memorandum, please contact me at (571) 212-6701, or Joe Nelson, Audit Manager, at (703) 562-6314.

cc: Sylvia W. Burns, CIOO
Zachary N. Brown, OCISO
Brandon Milhorn, COS and COO
Bret Edwards, CFO
Martin D. Henning, RMS
Mark Pearce, DCP
Brian Yellin, DOA
Daniel H. Bendler, DOA
Kimberly S. Teeples, DOA
John N. Conneely, CISR
E. Marshall Gentry, ORMIC

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

January 28, 2021

TO: Mark F. Mulholland
Assistant Inspector General for Information Technology Audits and Cyber
Office of Inspector General (OIG)

FROM: Doreen R. Eberley
Director
Division of Risk Management Supervision (RMS)

DOREEN EBERLEY Digitally signed by DOREEN EBERLEY Date: 2021.01.28 16:08:03 -05'00'

SUBJECT: Management Advisory Memorandum | Potential Exposure of Insured Institutions to the SolarWinds Compromise | No. 2021-001

Thank you for your January 22, 2021 advisory memorandum regarding the potential exposure of insured institutions to the SolarWinds compromise. In your advisory memorandum, you recount OIG's identification on December 17, 2020, of a decoded version of SolarWinds software that identified domain names (web sites) of entities possibly exposed to the compromise. The information specifically identified at least 11 financial institutions, including institutions that are insured by the FDIC.

The OIG did not assess the accuracy or completeness of the identified information, but shared it with FDIC officials late the evening of December 17, so that the FDIC could assess the information to determine whether it could be used to inform supervisory strategies in response to the SolarWinds compromise. Your January 22, 2021 advisory memorandum further requested that FDIC notify the OIG if the FDIC takes any actions in response to the information provided. This letter documents the FDIC's actions related to this information, including actions taken prior to and after receipt of the information shared by the OIG.

The morning of December 18, 2021, the FDIC compared the OIG's information to information received from [redacted] That same morning, RMS Cybersecurity and Critical Infrastructure Protection Specialist [redacted] contacted the OIG analyst who identified the information shared by the OIG with the FDIC to see if he had anything further to share. He did not.

Both sets of information identified a single state nonmember bank and a larger number of national and state member insured institutions. [redacted] also contacted her counterpart at the Office of the Comptroller of the Currency (OCC), who chairs the Federal Financial Institutions Examination Council (FFIEC), Task Force on Supervision, Cybersecurity and Critical Infrastructure Working Group (CCIWG) to confirm awareness. [redacted] The OCC CCIWG Chair had previously initiated the Crisis Communication Protocols in response to the broader breach. Through the CCIWG, the

Page 1 of 2

FDIC also coordinated action with the Board of Governors of the Federal Reserve System and the relevant state banking department for the lone state nonmember bank on the listings. [redacted]

[redacted] Although the public information suggested malicious actor targeting of the entities identified (consistent with the Category 3 definition in the Cybersecurity and Infrastructure Security Agency's Alert (AA20-352A)), we have not identified financial institutions or service providers that have observed activity consistent with that Category.

We are continuing to monitor the situation and appreciate the OIG sharing the information it identified.

cc: Sylvia W. Burns, CIOO
Zachary N. Brown, OCISO
Brandon Milhorn, COS and COO
Bret Edwards, CFO
Martin D. Henning, RMS
Mark Pearce, DCP
Brian Yellin, DOA
Daniel H. Bendler, DOA
Kimberly S. Teeples, DOA
John P. Conneely, CISR
E. Marshall Gentry, ORMIC

FDIC Federal Deposit Insurance Corporation

MEMO

TO: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

FROM: Brandon Milhorn
Digitally signed by BRANDON MILHORN
Date: 2021.11.07 10:20:10 -05'00'
Deputy to the Chairman, Chief Operating Officer, and Chief of Staff

CC: Doreen Eberley, Director RMS
Sylvia W. Burns, CIO
Zachary Brown, CISO
E. Marshall Gentry, CRO

DATE: November 5, 2021

RE: Management Response to the OIG Draft Audit Report, Sharing of Threat Information to Guide the Supervision of Financial Institutions (No. 2019-003)

The FDIC has completed its review of the Office of Inspector General's (OIG) draft audit report titled *Sharing of Threat Information to Guide the Supervision of Financial Institutions*, issued on October 5, 2021. FDIC management concurs with 22 of the report's 25 recommendations, partially concurs with 2 recommendations, and does not concur with 1 recommendation. Our responses to the audit findings and each recommendation are more fully described below.

We are particularly pleased that after two years of audit work conducted by multiple OIG staff members, numerous interviews, and extensive document review, the OIG's nearly 90-page audit report revealed no evidence that the FDIC failed to identify and properly disseminate any information relative to an identified threat to the FDIC or the financial system. Further, the OIG identified no instances where the FDIC inappropriately handled classified information. This notable positive outcome is a testament to the hard work, experience, and collaboration of the Senior Intelligence Officer (SIO), colleagues in the RMS Operational Risk Group and Office of the Chief Information Security Officer (OCISO), and threat information consumers across the FDIC.

The effectiveness of our existing program is demonstrated most clearly by our response to the SolarWinds compromise and the Kaseya ransomware attacks. In both instances, threat information was discovered, effectively disseminated throughout the FDIC, and communicated to financial institutions through established channels. Our threat information sharing program helped supplement a holistic response from the FDIC, from financial institution supervision to FDIC information technology, communications, legislative, and regional operations management. A description of each response, both of which occurred during the audit, provides some critical context on our existing threat information sharing operations.

Federal Deposit Insurance Corporation

The SolarWinds Response

From the beginning of the SolarWinds compromise,[1] the FDIC assessed and appropriately shared threat information internally to determine the impact on the Corporation, banks, and their service providers, and to inform our operational response. Despite the challenges presented by mandatory telework, our SIO provided 13 classified briefings to senior leadership and key stakeholders on the topic. Internal communications and talking points, informed by these classified briefings but at an unclassified level,[2] were disseminated throughout the organization, including to Regional Directors, regional offices, the Office of Communications, RMS, CISR, CIO and OCISO, the Office of Legislative Affairs, and to other affected organizations. Several meetings among senior leadership were conducted to coordinate the FDIC operational response. The FDIC also provided briefings to Congress and other relevant organizations on the impact of the event on the FDIC.

On December 16, 2020, to support financial institutions that could be affected by the incident, the FDIC amplified relevant alert and response information by linking to this unclassified information in an FDIC*connect* message to all insured depository institutions. On February 24, 2021, the FDIC sent another FDIC*connect* message to insured depository institutions that contained information about the compromise along with resources to assist with threat monitoring, response activities, and risk assessment. The FDIC also shared this information with the most significant bank service providers. Further, FDIC officials directly contacted institutions potentially more vulnerable to the compromise to confirm they had taken appropriate remediation steps. The FDIC also provided alerts and multiple technical briefings to IT examiners and leaders so that they had relevant contextual information as they interacted with banks and service providers on this event.

By taking these actions, the FDIC ensured that it understood the operational and supervisory impact of the compromise, that examiners were well-informed about the potential impact and how a company should address the compromise, that financial institutions and their service providers were remediating risk, that the FDIC was aware of any significant compromises or disruptions of financial services, and that appropriate internal actions were taken to ensure the security and continuity of FDIC operations. During the audit, OIG staff verbally acknowledged that the FDIC's response efforts and sharing of intelligence information were effective and appropriate. SolarWinds is an example that demonstrates the FDIC has effective processes to acquire, analyze, disseminate and use relevant and actionable threat information, including classified information, to guide the supervision of financial institutions and protect FDIC operations.

The Kaseya Response

The FDIC's handling of the Kaseya Corporation compromise offers another noteworthy example of the FDIC's effectiveness in responding to a cyberattack. Kaseya Corporation, a security and IT management service provider with roughly 40,000 customers worldwide (including financial services companies), confirmed a ransomware attack in early July 2021 on its VSA product line. VSA is a network security tool designed to automate patch management, endpoint management, and network monitoring. The threat actors leveraged a

[1] On December 13, 2020, SolarWinds, a Texas-based global provider of IT infrastructure management software, communicated with Orion Platform products customers about a cyberattack that inserted a vulnerability into those products.

[2] Section 1.6(g) of Executive Order 13526, Classified National Security Information, describes the importance of disseminating information "at the lowest level of classification possible or in unclassified form." Sharing threat information at the lowest classification level possible provides for increased distribution and, as such, facilitates a more effective operational response.

MEMO 2

FDIC Federal Deposit Insurance Corporation

vulnerability in the Kaseya VSA software to attack the users of Kaseya's on-premise products and their downstream customers.

Once aware of the incident, the FDIC again analyzed and shared threat information internally so that it could assess the impact on the Corporation, banks, and their service providers, and take appropriate action based on those assessments. [redacted] Regional office staff [redacted] contacted companies to determine the level of impact and remediation steps taken.

Beyond the SolarWinds and Kaseya events, there are additional examples of effective threat information sharing, including classified information sharing, that the FDIC discussed on multiple occasions with OIG staff.

Response to the OIG Audit

We generally agree that the OIG's recommended control enhancements have merit, such as better documenting existing processes and procedures for threat information sharing and building a more robust community of practice for threat information analysis and dissemination across the FDIC.

Based on the March 2021 SIO briefing on the status of the FDIC's intelligence support program, the Chief Operating Officer (COO) directed a review of our intelligence and insider threat programs. Based on this review and ongoing discussions with the OIG related to this audit, the FDIC established a new Intelligence and Threat Sharing Group (ITSG) in October 2021. Once staffed, the ITSG will report directly to a newly established Chief of Staff to the COO. Centralizing and elevating these important functions will help enhance focus and coordination among intelligence sharing, counterintelligence, and insider threat responsibilities. Led by a newly established Corporate Manager, the ITSG will develop a group charter and standard operating procedures over the next year, and coordinate a network of liaisons from key Divisions and Offices to increase the communities of practice associated with threat information analysis and dissemination across the FDIC.

Throughout its draft report, the OIG is critical of the FDIC for relying on the judgment and discretion of its employees to manage the analysis and dissemination of threat information. The OIG recommends procedures to address this concern. The analysis and dissemination of threat information necessarily relies on the exercise of individual judgement by analysts informed by their training, knowledge, and experience. Our SIO [redacted] and the RMS Operational Risk team (38 employees with approximately 20 years tenure each for a cumulative 760 years of experience working with threat information in a supervisory context) have exactly the type of training, knowledge, and experience that allows the FDIC to rely on their *collective* expertise to analyze and appropriately disseminate threat information (including classified information), formulate recommendations, lead important projects, and support leadership on numerous initiatives. While the FDIC agrees that additional formal processes and procedures will support their efforts, the OIG found no evidence during the audit that these qualified and experienced professionals failed to effectively perform their duties.

In its report, the OIG stated, in part: "A primary reason the Regional Directors did not receive classified information was because the FDIC had not established the necessary infrastructure to enable the dissemination or receipt of classified information in its regional office locations." The FDIC disagrees with the OIG's conclusions on this point.

First, the FDIC has coordinated through the U.S. Department of the Treasury to use other agency Sensitive

Federal Deposit Insurance Corporation

Compartmented Information Facilities (SCIFs) outside of Washington D.C. for FDIC employees to participate in classified briefings when needed. As necessary, we can engage with Treasury to utilize these facilities to inform an operational response.[3]

Second, FDIC management experience suggests that classified briefings and intelligence dissemination are generally unnecessary for Regional Directors to effectively understand threat information.[4] With regard to any particular threat, classified information may broaden FDIC's understanding and inform any proposed operational response, but it is rarely the sole source of threat information and does not generally change the FDIC's operational or supervisory response or affect response guidance provided to field staff. In infrequent instances where classified information has led to changes to the FDIC's supervisory response, that information has been reviewed at headquarters, and unclassified information used to explain the reason for the change to field staff.

Third, consistent with Executive Order 13526, the FDIC's goal is the dissemination of threat information at the lowest classification level possible or at an unclassified level.[5] In general, we have found that information necessary to inform a supervisory or operational response is best shared at the unclassified level – to support broader and more rapid information sharing, particularly with FDIC field staff and financial institution employees that lack clearances. Even in cases where extremely sensitive classified information relates to a potential operational threat or a threat to the financial system, our experience suggests that unclassified threat information sharing is preferred and sufficient to execute an effective operational and supervisory response.[6]

Management Response to the OIG Recommendations

Recommendation 1: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Establish, approve, and implement a Charter to govern the acquisition, analysis, and dissemination of threat information under the FDIC's Intelligence Support Program.

Management Decision: Concur

Planned Action:

The newly established ITSG will establish and implement, in coordination with the Legal Division, an approved Charter to govern the acquisition, analysis, and dissemination of threat information as part of the FDIC's intelligence support functional area. These efforts will include articulation of standard operating procedures,

[3] For example, a senior examination specialist has used another agency's SCIF in Arizona to receive classified information about particular threats during 2021.
[4] This is not to imply that the requirement for Regional Directors to obtain TS/SCI security clearances is inappropriate. Indeed, there could be legitimate Continuity of Operations (COOP) and Continuity of Government (COG) reasons to maintain the requirement, along with the potential need to share classified threat information with the Regional Directors when necessary to understand and respond to a potential threat. See the response to Recommendation 15 below.
[5] Executive Order 13526 (December 29, 2009), and available at https://www.archives.gov/isoo/policy-documents/cnsi-eo.html. See Sections 1.6(g) and 2.1(c).
[6] See, for example, the SolarWinds response discussed above.

FDIC Federal Deposit Insurance Corporation

other guidance documents, and associated performance metrics relative to threat information sharing.

Estimated Completion Date: June 30, 2022

Recommendation 2: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Establish and implement performance goals, objectives, and measures to govern and assess the threat sharing activities performed under the FDIC's Intelligence Support Program.

Management Decision: Concur

Planned Action:

See response to Recommendation 1.

Estimated Completion Date: June 30, 2022

Recommendation 3: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer coordinate with the FDIC Legal Division to:

Establish and implement policies and procedures that define roles and responsibilities for acquiring, analyzing, and disseminating threat information under the FDIC's Intelligence Support Program.

Management Decision: Concur

Planned Action:

See response to Recommendation 1.

Estimated Completion Date: June 30, 2022

Recommendation 4: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer coordinate with the FDIC Legal Division to:

Establish and implement policies and procedures governing the use of national intelligence to conduct background investigations of foreign nationals listed on applications for Federal Deposit Insurance and Notices of Change in Control.

Management Decision: Concur

Planned Action:

The COO organization will coordinate with the Legal Division and RMS to establish and implement policies and procedures governing the use of national intelligence to conduct background investigations of foreign nationals listed on applications for Federal Deposit Insurance and Notices of Change in Control.

Estimated Completion Date: June 30, 2022

MEMO 5

Federal Deposit Insurance Corporation

Recommendation 5: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer coordinate with the FDIC Legal Division to:

Establish and implement policies and procedures to govern the activities of the FDIC Federal Senior Intelligence Coordinator.

Management Decision: Concur

Planned Action:

See response to Recommendation 1.

Estimated Completion Date: June 30, 2022

Recommendation 6: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer coordinate with the FDIC Legal Division to:

Establish and implement policies and procedures for developing, approving, and maintaining the Information Needs Document.

Management Decision: Concur

Planned Action:

As part of the policies and procedures document discussed in response to Recommendation 1, the newly established ITSG will include provisions for developing, approving, and maintaining the Information Needs Document.

Estimated Completion Date: June 30, 2022

Recommendation 7: We recommend that the Director, RMS, coordinate with the Legal Division to:

Define roles and responsibilities for RMS threat information sharing activities.

Management Decision: Concur

Planned Action:

In coordination with the ITSG and the Legal Division, RMS will document the defined roles and responsibilities for RMS threat information sharing activities such as for updating the RMS cyber incident response procedures, and for acquiring, analyzing, and disseminating threat information.

Estimated Completion Date: March 31, 2022

Recommendation 8: We recommend that the Director, RMS, coordinate with the Legal Division to:

Establish and implement procedures for RMS threat information sharing activities.

Management Decision: Concur

MEMO 6

Federal Deposit Insurance Corporation

Planned Action:

See response to Recommendation 7.

Estimated Completion Date: June 30, 2022

Recommendation 9: We recommend that the Chief Risk Officer:

Ensure that FDIC Enterprise Risk Inventory and Risk Profile fully consider the threat information sharing risks identified in this report.

Management Decision: Concur.

Planned Action: The existing Risk Inventory and Risk Profile contain risk items directly related to protecting and disseminating classified information, succession planning, responding to IT and cybersecurity risk in banks and technology service providers, information sharing, and maintaining strong internal controls. The Office of Risk Management and Internal Controls will perform a risk assessment to confirm that enterprise risks related to threat information sharing are accurately reflected.

Estimated Completion Date: December 20, 2021

Recommendation 10: We recommend that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff:

Update and approve the Information Needs Document to incorporate input from all relevant Divisions and Offices regarding their threat information requirements.

Management Decision: Concur

Planned Action:

See response to Recommendation 6.

Estimated Completion Date: June 30, 2022

Recommendation 11: We recommend that the Director, RMS:

Finalize and implement a requirement for FDIC-supervised financial institutions to promptly report destructive cyber incidents to the FDIC.

Management Decision: Concur, pending Board action

Planned Action:

The FDIC is working with the other bank regulators to consider comments received regarding a computer security incident notification Notice of Proposed Rulemaking (NPR) published in January 2021. The FDIC Board of Directors has sole discretion on whether or not this rule will be finalized and implemented. The FDIC Board of Directors decision will consider the comments received on the NPR.

MEMO 7

FDIC Federal Deposit Insurance Corporation

If the FDIC Board approves a final rule, FDIC staff will implement the rule by creating and deploying processes to receive notifications, analyze them, and take any appropriate action. FDIC will also train staff on, and inform banks of, these processes.

Estimated Completion Date: Pending FDIC Board approval

Recommendation 12: We recommend that the Director, RMS:

Ensure threat analysis includes relevant trends, patterns, and emerging issues facing financial institutions, including analysis of RMS data.

Management Decision: Partially Concur

Planned Action:

RMS will continue to ensure threat analysis includes relevant trends, patterns, and emerging issues facing financial institutions. RMS will continue to analyze Suspicious Activity Reports (SARs) as the best source for information regarding cyber attacks against FDIC-supervised financial institutions. RMS may augment analysis of cyber incidents reported in SARs with other information, including information obtained at examinations. If the FDIC Board of Directors approves a computer security incident notification rule, RMS will establish processes to receive notifications, analyze them, and take any appropriate action.

Estimated Completion Date: Pending FDIC Board approval of any computer security incident notification rule

Recommendation 13: We recommend that the Director, RMS, and the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Establish and implement a means to share classified information with the Regional Offices in a timely manner so that it is actionable.

Management Decision: Concur

Planned Action:

Consistent with Executive Order 13526, the FDIC will continue to share actionable threat information with Regional Offices in a timely manner and at the lowest classification level possible to understand the information, with a strong preference for unclassified information sharing. The FDIC will coordinate with Treasury to formalize an arrangement to use other agency SCIFs, if needed.

Estimated Completion Date: March 31, 2022

Recommendation 14: We recommend that the Director, RMS, and the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Establish a means for Regional Offices to handle classified information once it is shared, including the infrastructure (systems, facilities, and communications) to securely handle, transmit, discuss, store, and dispose of classified information.

Management Decision: Do Not Concur

MEMO 8

FDIC Federal Deposit Insurance Corporation

Planned Action:

Consistent with FDIC management experience associated with threat information sharing and the guidance provided in Executive Order 13526, the construction of SCIFs and other associated infrastructure in our Regional Offices is not justified at this time given the significant costs of establishing and maintaining the facilities and the successful sharing of threat information at unclassified levels with Regional Directors and field staff. The FDIC will continue to coordinate with Treasury to use other agency SCIFs, if needed.

Estimated Completion Date: N/A

Recommendation 15: We recommend that the Director, RMS, and the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Evaluate and document whether additional Regional Office personnel should be required to hold a security clearance based on business needs.

Management Decision: Concur

Planned Action:

The FDIC will re-evaluate and document whether any Regional Directors or other Regional Office personnel should be required to hold a security clearance and, if so, at what level. Particularly with respect to other Regional Office Personnel, FDIC management experience suggests that it is unlikely that such clearances will be necessary for routine classified briefings as the FDIC has effectively shared threat information at unclassified levels without inhibiting operational or supervisory responses or further information sharing.[7] Regional Directors will be evaluated separately given COOP/COG considerations and other potential operational and supervisory requirements.

Estimated Completion Date: March 31, 2022

Recommendation 16: We recommend that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff and the Director, RMS:

Establish and implement a procedure to measure the utility and effectiveness of threat information used to support the supervision program.

Management Decision: Concur

Planned Action:

The FDIC will document its procedures for measuring the utility and effectiveness of threat information used to support the supervision program, and consider adding to these procedures if necessary.

Estimated Completion Date: June 30, 2022

[7] Executive Order 13526 (December 29, 2009), and available at https://www.archives.gov/isoo/policy-documents/cnsi-eo.html. See Sections 1.6(g) and 2.1(c).

MEMO 9

Federal Deposit Insurance Corporation

Recommendation 17: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Establish a backup for the SIO to ensure the continued implementation of key duties and responsibilities.

Management Decision: Concur

Planned Action:

The ITSG intends to establish a network of liaisons in key Divisions and Offices that will add resilience to the FDIC's threat information sharing program, including its ability to analyze and appropriately disseminate threat information derived from classified intelligence.

Estimated Completion Date: March 31, 2022

Recommendation 18: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Establish a succession plan to addresses a potential departure of the SIO.

Management Decision: Partially Concur

Planned Action:

The COO organization's newly established ITSG will be staffed with several new professional level personnel. When staffing this new organization, the COO organization will ensure sufficient bench strength and backup support to the SIO position. Further, a team of liaisons embedded within key Divisions and Offices will provide an extra layer of resiliency to support the SIO when needed.

Estimated Completion Date: March 31, 2022

Recommendation 19: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Require that the SIO maintain unclassified threat information on a centralized storage platform so that it would be accessible by other FDIC personnel with a business need.

Management Decision: Concur

Planned Action:

The FDIC has established a centralized storage site for all unclassified intelligence support function files and records that is accessible to FDIC personnel with a business need. We will continue to require unclassified threat information be maintained on this centralized platform and ensure that it is accessible by other FDIC personnel with a business need.

Estimated Completion Date: Completed

Recommendation 20: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating

Federal Deposit Insurance Corporation

Officer:

Establish minimum training requirements for the SIO consistent with the SIO's responsibilities.

Management Decision: Concur

Planned Action:

The COO organization will establish a training framework for ITSG personnel and liaison officers that support the group.

Estimated Completion Date: June 30, 2022

Recommendation 21: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Implement measures to ensure that SEPS processes requests for security clearances submitted by Divisions and Offices in a timely manner.

Management Decision: Concur

Planned Action:

During 2021, the COO organization implemented a number of processes and eWORKS enhancements to ensure employee background investigations are submitted and completed in a timely manner. These enhancements will result in more timely security clearances as well. We will continue to ensure that SEPS processes requests for security clearances in a timely manner and Administrative Officers promptly inform SEPS when employees enter into new positions that require a security clearance.

Estimated Completion Date: Completed

Recommendation 22: We recommend that the Deputy to the Chairman, Chief of Staff, and Chief Operating Officer:

Implement measures to ensure that Administrative Officers promptly inform SEPS when employees enter into new positions that require a security clearance.

Management Decision: Concur

Planned Action:

Please see response to recommendation 21.

Estimated Completion Date: Completed

Recommendation 23: We recommend that the CIO:

Establish a process to ensure that the CDM maintains current information regarding the information types used by the FDIC.

MEMO 11

Federal Deposit Insurance Corporation

Management Decision: Concur

Planned Action:

The Chief Data Officer Staff (CDOS) will establish a process to ensure that the Conceptual Data Model (CDM) maintains current information and is regularly updated.

Estimated Completion Date: September 30, 2022

Recommendation 24: We recommend that the CIO:

Categorize the unclassified threat information managed by the SIO and include this information in the CDM.

Management Decision: Concur

Planned Action:

The CDOS will work with the SIO to understand the existing scope of unclassified threat information. The CDOS will ensure that this information is properly categorized and mapped under the CDM

Estimated Completion Date: September 30, 2022

Recommendation 25: We recommend that the CIO:

Ensure that appropriate security controls are implemented to protect unclassified threat information by the SIO consistent with NIST guidance.

Management Decision: Concur

Planned Action:

The OCISO will coordinate with the DOA Information Security Manager to (1) determine whether security controls for protecting unclassified threat information managed by the SIO are commensurate with the security categorization assigned in response to Recommendation 24 and (2) implement any additional security controls needed to adequately protect this information.

Estimated Completion Date: December 16, 2022

MEMO 12

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 newly established ITSG will establish and implement, in coordination with the Legal Division, an approved Charter to govern the acquisition, analysis, and dissemination of threat information as part of the FDIC's intelligence support function area. The efforts will include articulation of standard operating procedures, other guidance documents and associated performance metrics relative to threat information sharing.	June 30, 2022	$0	Yes	Open
2	See response to Recommendation 1.	June 30, 2022	$0	Yes	Open
3	See response to Recommendation 1.	June 30, 2022	$0	Yes	Open
4	The COO organization will coordinate with the Legal Division and RMS to establish and implement policies and procedures governing the use of national intelligence to conduct background investigations of foreign nationals listed on applications for Federal Deposit Insurance and Notices of Change in Control.	June 30, 2022	$0	Yes	Open
5	See response to Recommendation 1.	June 30, 2022	$0	Yes	Open
6	As part of the policies and procedures document discussed in response to Recommendation 1, the newly established ITSG will include provisions for developing, approving, and maintaining the Information Needs Document.	June 30, 2022	$0	Yes	Open
7	In coordination with the ITSG and the Legal Division, RMS will document the defined roles and responsibilities for RMS threat information sharing activities such as for updating the RMS cyber incident response procedures, and for acquiring, analyzing, and disseminating threat information.	March 31, 2022	$0	Yes	Open
8	See response to Recommendation 7.	June 30, 2022	$0	Yes	Open
9	The existing Risk Inventory and Risk Profile contain risk items directly related to protecting and disseminating classified information, succession planning, responding to IT and cybersecurity risk in banks and technology service providers, information sharing, and maintaining	December 20, 2021	$0	Yes	Open

	strong internal controls. The Office of Risk Management and Internal Controls will perform a risk assessment to confirm that enterprise risks related to threat information sharing are accurately reflected.				
10	See response to Recommendation 6.	June 30, 2022	$0	Yes	Open
11	The FDIC is working with the other bank regulators to consider comments received regarding a computer security incident notification Notice of Proposed Rulemaking (NPR) published in January 2021. The FDIC Board of Directors has sole discretion on whether or not this rule will be finalized and implemented. The FDIC Board of Directors' decision will consider the comments received on the NPR.	Pending FDIC Board Approval	$0	Yes	Open
12	RMS will continue to ensure threat analysis includes relevant trends, patterns, and emerging issues facing financial institutions. RMS will continue to analyze Suspicious Activity Reports (SARs) as the best source for information regarding cyber attacks against FDIC-supervised financial institutions. RMS may augment analysis of cyber incidents reported in SARs with other information, including information obtained at examinations. If the FDIC Board of Directors approves a computer security incident notification rule, RMS will establish processes to receive notifications, analyze them, and take appropriate action.	Pending FDIC Board approval of any computer security incident notification rule.	$0	Yes	Open
13	Consistent with Executive Order 13526, the FDIC will continue to share actionable threat information with Regional Offices in a timely manner and at the lowest classification level possible to understand the information, with a strong preference for unclassified information sharing. The FDIC will coordinate with Treasury to formalize an arrangement to use other agency SCIFs, if needed.	March 31, 2022	$0	Yes	Open
14	The FDIC non-concurred with this recommendation. It is considered unresolved, and we will seek resolution during the evaluation follow-up process.	TBD	$0	No	Open

15	The FDIC will re-evaluate and document whether any Regional Directors or other Regional Office personnel should be required to hold a security clearance and, if so, at what level. Particularly with respect to other Regional Office personnel, FDIC management experience suggests that it is unlikely that such clearances will be necessary for routine classified briefings as the FDIC has effectively shared threat information at unclassified levels without inhibiting operational or supervisory responses or further information sharing. Regional Directors will be evaluated separately given COOP/COG considerations and other potential operational and supervisory requirements.	March 31, 2022	$0	Yes	Open
16	The FDIC will document its procedures for measuring the utility and effectiveness of threat information used to support the supervision program, and consider adding to these procedures if necessary.	June 30, 2022	$0	Yes	Open
17	The ITSG intends to establish a network of liaisons in key Divisions and Offices that will add resilience to the FDIC's threat information sharing program, including its ability to analyze and appropriately disseminate threat information derived from classified intelligence.	March 31, 2022	$0	Yes	Open
18	The COO organization's newly established ITSG will be staffed with several new professional level personnel. When staffing this new organization, the COO organization will ensure sufficient bench strength and backup support to the SIO position. Further, a team of liaisons embedded within key Divisions and Offices will provide an extra layer of resiliency to support the SIO when needed	March 31, 2022	$0	Yes	Open
19	The FDIC has established a centralized storage site for all unclassified intelligence support function files and records that is accessible to FDIC personnel with a business need. The FDIC will continue to require unclassified threat information be maintained on this central platform and ensure that it is accessible by other FDIC personnel with a business need.	Completed	$0	Yes	Closed

20	The COO organization will establish a training framework for ITSG personnel and liaison officers that support the group.	June 30, 2022	$0	Yes	Open
21	During 2021, the COO organization implemented a number of processes and eWORKS enhancements to ensure employee background investigations are submitted and completed in a timely manner. These enhancements will result in more timely security clearances as well. The FDIC will continue to ensure that SEPS processes requests for security clearances in a timely manner and Administrative Officers promptly inform SEPS when employees enter into new positions that require a security clearance.	Completed	$0	Yes	Open
22	See response to Recommendation 21.	Completed	$0	Yes	Open
23	The Chief Data Officer Staff (CDOS) will establish a process to ensure that the Conceptual Data Model (CDM) maintains current information and is regularly updated.	September 30, 2022	$0	Yes	Open
24	The CDOS will work with the SIO to understand the existing scope of unclassified threat information. The CDOS will ensure that this information is properly categorized and mapped under the CDM.	September 30, 2022	$0	Yes	Open
25	The OCISO will coordinate with the DOA Information Security Manager to (1) determine whether security controls for protecting unclassified threat information managed by the SIO are commensurate with the security categorization assigned in response to Recommendation 24 and (2) implement any additional security controls needed to adequately protect this information.	December 16, 2022	$0	Yes	Open

[a] Recommendations are resolved when —

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

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

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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