Sharing of Threat and Vulnerability Information with Financial Institutions

August 2023 **EVAL-23-002**

Evaluation 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.

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Notice

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

Office of Inspector General

Executive Summary

Sharing of Threat and Vulnerability Information with Financial Institutions

Financial institutions face a wide range of significant and persistent threats to their operations. Such threats include cyberattacks, money laundering, terrorist financing, pandemics, and natural disasters such as hurricanes, tornadoes, and floods. Whether man-made or natural, these threats can disrupt the delivery of financial services and inflict financial harm on consumers and businesses. The interconnected nature of the financial services industry further elevates the potential impact that threats can have on financial institutions. For example, many insured financial institutions rely on third-party service providers to provide critical banking services. An incident at a large service provider could have a cascading impact on a large number of financial institutions. If widespread, the impact could ultimately diminish public confidence and threaten the stability of the United States financial system.

To fulfill its mission, the Federal Deposit Insurance Corporation (FDIC) acquires, analyzes, and disseminates threat information relating to cyber and other threats both internally and to the financial sector. Sharing threat information that the FDIC uniquely develops or summarizes, 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.

To assess the FDIC's efforts in the sharing of threat information to guide the supervision of financial institutions (internal sharing), we completed the first phase of this assignment in January 2022. Our audit report entitled, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (January 2022), identified that the FDIC had not established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The report contained 25 recommendations to improve the FDIC's threat sharing operations. In response to our findings, in October 2021, the FDIC established the Intelligence and Threat Sharing Unit (ITSU) to centralize the FDIC's threat intelligence functions. The ITSU coordinates with a network of liaisons from key FDIC Divisions and Offices to increase the communities of practice associated with threat information analysis and dissemination across the FDIC. To support ITSU operations, the FDIC established, the Intelligence Support

Program (ISP) within DOA to coordinate threat information acquisition, analysis, and production.

The Operational Risk group within the Division of Risk Management Supervision (RMS) works to identify, monitor, and analyze information about operational risks that can threaten the safety and soundness of FDIC-supervised financial institutions. As such, the FDIC has identified the Operational Risk group within RMS as the responsible entity for communicating threat information externally with financial institutions.

We initiated the second phase of the assignment to focus on the FDIC's sharing of threat information externally with financial institutions. Specifically, our evaluation objective was to determine whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information.

Results

The FDIC has implemented processes for the sharing of threat and vulnerability information with financial institutions. For example, the FDIC established formal procedures to communicate cyber threat and vulnerability information. However, the FDIC can improve the effectiveness of its processes to ensure financial institutions receive actionable and relevant threat and vulnerability information. We determined that:

- The FDIC can improve its sharing of threat and vulnerability information with financial institutions and other financial sector entities;
- The FDIC can improve its controls over the recording of computer-security incidents to support threat intelligence operations and sharing activities;
- The FDIC can mature its threat information sharing program by establishing procedures for sharing non-cyber related threat information and revising the program's existing threat sharing policies and procedures; and
- The FDIC can enhance its capabilities to identify threat and vulnerability information.

With these improvements, the FDIC will be better positioned to effectively share accurate, complete, and relevant threat and vulnerability information with financial institutions.

The FDIC, as a member of the Federal Financial Institutions Examination Council (FFIEC), has jointly stated that financial institutions should have an effective threat intelligence program, including methods for gathering, monitoring, sharing, and responding to threat and vulnerability information in order to support their safety and soundness. According to FDIC officials, other U.S. government and private sector entities are proficient at providing threat information to financial institutions. As a result, FDIC officials stated that the sharing of this same information is unnecessary. The FDIC, however, was created by Congress to maintain stability and public confidence in the Nation's financial system. The FDIC can further this mission by sharing threat information that the FDIC uniquely develops or summarizes to be specifically relevant to financial institutions. Specifically, information sharing improves financial institutions' ability to detect, respond, assess, or focus on threats and vulnerabilities relevant to their operations.

Recommendations

This report contains 10 recommendations to improve the FDIC's processes in order to ensure that financial institutions receive actionable and relevant threat and vulnerability information. We recommend that the FDIC share FDIC-developed threat and vulnerability information with financial institutions or other financial sector entities, improve controls over the recording of computer-security incidents reported by banks and service providers, and ensure computer-security incident information in Virtual Supervisory Information on the Net (ViSION) and within RMS Incident Reports is complete, appropriate, and accurate. We also recommend that the FDIC mature its threat intelligence operations by establishing procedures for sharing non-cyber related threat information and revising the program's existing policies and procedures. In addition, we recommend that the FDIC develop performance measures for its external threat sharing activities. We also recommend that the FDIC enhance its threat intelligence operations by ensuring all data sets within the FDIC that contain relevant threat and vulnerability information are assessed to support threat and vulnerability information sharing operations.

The FDIC concurred with all 10 recommendations in this report and plans to complete all corrective actions by March 31, 2024.

Contents

August 29, 2023

Subject | ***Sharing of Threat and Vulnerability Information with Financial Institutions***

The Federal Deposit Insurance Corporation (FDIC) was created by Congress to maintain stability and public confidence in the Nation's financial system. To accomplish this mission, the FDIC insures deposits, examines and supervises financial institutions[1] for safety and soundness and consumer protection, makes large and complex financial institutions resolvable, and manages receiverships.[2] As of December 31, 2022, the FDIC insured approximately $17.7 trillion in deposits at 4,706 commercial banks and savings institutions.[3] The FDIC also served as the primary Federal regulator for 3,032 of these institutions, and the backup regulator for the remaining 1,674 institutions.

Such financial institutions face a wide range of significant and persistent threats to their operations. Such threats include cyberattacks, money laundering, terrorist financing, pandemics, and natural disasters. Whether man-made or natural, these threats can disrupt the delivery of financial services and inflict financial harm on consumers and businesses. 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 to 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 help fulfill its mission and protect the stability of the Nation's financial system, the FDIC acquires, analyzes, and disseminates[4] threat information relating to cyber events and other threats to the financial sector and FDIC operations. Effective

[1] For the purposes of the report, a financial institution represents an FDIC-insured depository institution. The word bank is used interchangeably with financial institution throughout this report.
[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. Chapter 53.
[3] FDIC *Quarterly Banking Profile* (Fourth Quarter 2022).
[4] The word disseminate is used interchangeably with the word share throughout this report.

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, including the Division of Administration (DOA) and the Division of Risk Management Supervision (RMS).

Our evaluation objective was to determine whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information. We conducted this evaluation from August 2022 through July 2023 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). Appendix 1 of this report provides additional details about our objective, scope, and methodology.

BACKGROUND

In January 2022, we issued an audit report on the FDIC's *Sharing of Threat Information to Guide the Supervision of Financial Institutions*.[5] This was the first report in a series of two that focused on the FDIC's sharing of threat information. The audit found that the FDIC had not established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The report contained 25 recommendations to improve the FDIC's internal threat sharing operations.

In response to the audit findings, the FDIC established the Intelligence and Threat Sharing Unit (ITSU)[6] in October 2021, and hired the ITSU Chief in August 2022. The DOA also issued FDIC Directive 1600.09 in December 2022 to provide policy, assign responsibilities, and prescribe processes for the acquisition, analysis, production, and dissemination of "all-hazard threat information" under the FDIC's Intelligence Support Program (ISP).[7] The ITSU's ISP is responsible for coordinating threat information acquisition, analysis, and production for the FDIC. This includes determining the threat information needs of FDIC Divisions and Offices,[8] identifying relevant threat information databases and sources, and sharing DOA ITSU-authored and other agency-authored intelligence products aligned to the FDIC's threat information needs with FDIC stakeholders.[9]

[5] FDIC Office of Inspector General (OIG), *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (AUD-22-003) (January 2022).

[6] The FDIC first established the group as the Intelligence and Threat Sharing Group and reorganized and renamed it as the ITSU.

[7] FDIC Directive 1600.09, *Intelligence and Counterintelligence Programs (*December 2022).

[8] In December 2022, the FDIC's ITSU established its Calendar Year (CY) 2023 Standing Information Needs and Key Intelligence Questions.

[9] According to the FDIC's Standard Operating Procedure for Threat Information Acquisition, Analysis, Production, Dissemination, and Storage, a stakeholder is defined as any FDIC Division, Office, or employee who has a threat information need to support and inform decision making, operations, or knowledge base/situational awareness.

The Operational Risk group within 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 response to the January 2022 Office of Inspector General (OIG) audit report, RMS finalized and implemented the RMS Threat and Vulnerability Communication Operating Procedures (RMS Threat Communication Operating Procedures), to provide a common methodology for determining whether threat or vulnerability information should be communicated by RMS to FDIC-supervised insured depository institutions, examined service providers, or supervisory personnel. As described in this report, the RMS Threat Communication Operating Procedures were only intended to focus on and apply to cyber and computer-security related threats and vulnerabilities. Other FDIC Divisions, including the Chief Information Officer Organization (CIOO), Division of Depositor and Consumer Protection (DCP), and Division of Complex Institution Supervision and Resolution (CISR) may also receive threat and vulnerability information through their operations that RMS may share with financial institutions.

Threats Against Financial Institutions

Financial institutions face an evolving and dynamic set of operational threats, including cyberattacks; fraud and financial crimes; pandemics; and natural disasters such as hurricanes, tornadoes, and floods.

Cyberattacks. In January 2020, the FDIC and the Office of the Comptroller of Currency (OCC) issued a Joint Statement on Heightened Cybersecurity Risk which stated that disruptive and destructive cyberattacks against financial institutions have increased in frequency and severity in recent years. According to this Joint Statement, threat actors often use destructive malware[10] to exploit weaknesses in information systems at financial institutions. The Joint Statement 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. Further, in 2022, the FDIC issued a report on Cybersecurity and Resilience, which states that the fight against malicious actors who use cyberspace to harm others requires constant vigilance and agility.

Fraud and Financial Crimes. The risk of fraud and financial crime continue to escalate despite all of the efforts taken to mitigate risks.[11] The OCC specifically warns that financial crime threatens the safety and soundness of financial systems world-wide. The OCC reports that, in some cases, these crimes threaten the security and safety of the nation. In addition, the OCC describes that these crimes

[10] Malware is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
[11] Why Banks and Finance Organisations are Orchestrating the Risk of Financial Crime and Fraud (November 2022).

range from fairly simple operations carried out by individuals or small groups to highly sophisticated rings seeking funding for criminal enterprises or terrorism.

Money Laundering. In February 2022, the United States Department of the Treasury (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. The United States is particularly vulnerable to all forms of illicit finance because of the size of the U.S. financial system and the centrality of the U.S. dollar in the payment infrastructure supporting global trade. Financial institutions are responsible for developing and administering a program to assure and monitor compliance with the Bank Secrecy Act (BSA)—a statute intended to facilitate the detection and prevention of money laundering.[12]

Terrorist Financing. In October 2015, the Financial Action Task Force (FATF) issued a report, entitled *Emerging Terrorist Financing Risks*.[13] 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. According to the *2022 National Terrorist Financing Risk Assessment,*[14] U.S. authorities have made significant progress in addressing some of the key vulnerabilities terrorist groups have been able to exploit. By developing deep expertise on terrorist financing threats and vulnerabilities, building a robust legal and operational architecture, and strengthening international relationships and institutions, the United States has degraded the financial and support networks for a range of terrorist groups. Moreover, the USA PATRIOT Act created a legal framework for the U.S. government to share information and help financial institutions better identify and report terrorist financing activity, as well as for financial institutions to share information amongst themselves when they have a reasonable basis to believe that the information shared relates to activities that may involve terrorist activity.

Pandemics. In January 2020, the World Health Organization declared the outbreak of a novel coronavirus—Coronavirus Disease—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)[15] Annual Report for

[12] The BSA 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.
[13] The FATF sets international standards that aim to prevent money laundering and terrorist financing and the harm they cause to society. FATF Report on Emerging Terrorist Financing Risks (October 2015).
[14] Treasury Department, 2022 National Terrorist Financing Risk Assessment (February 2022).
[15] The Dodd-Frank Act created FSOC. 12 U.S.C. § 5321. 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. 12 U.S.C. § 5322.

2020 described the global pandemic caused by Coronavirus Disease as "the biggest external shock to hit the post-war U.S. economy."

Natural Disasters. According to a 2021 Report on Climate-Related Financial Risk[16] by FSOC, the financial sector will face evolving operational risks from the impact of climate change on the infrastructure required to maintain orderly sector operations. While the financial services sector has invested in business continuity, developed disaster recovery plans, and maintained robust capabilities to sustain critical operations during natural disasters, climate change is projected to increase the likelihood and severity of extreme weather events across the country, putting new strains on the critical infrastructure—both within and outside the financial services sector—necessary to maintain financial operations and financial stability. In addition, according to a Department of Homeland Security (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.

Sources of Threat Information

There are numerous sources of information available to support the FDIC's sharing of threat and vulnerability information both internally with FDIC operational components and externally with banks. These sources may also support a bank's threat intelligence operation. See Table 1 below for a summary of common threat information sources and examples.

[16] FSOC, Report on Climate-Related Financial Risk (October 21, 2021).

Table 1: Sources of Threat Information

Source	Examples
Media	News outlets Social media sites Blogs, bulletin boards, other forums available to the general public
Commercial Vendors	Financial Services Information Sharing and Analysis Center (FS-ISAC) FireEye Mandiant
Federal Agencies	Treasury Department, including the Financial Crimes Enforcement Network (FinCEN) DHS, including the Cybersecurity and Infrastructure Security Agency (CISA) The Federal Bureau of Investigation (FBI) and other Intelligence Community members Federal Banking Agencies, including the FDIC, the OCC, and the Board of Governors of the Federal Reserve System (FRB)
Federal Governance Bodies	Financial and Banking Information Infrastructure Committee (FBIIC) Federal Financial Institutions Examination Council (FFIEC)
Others	Financial Institutions Financial Industry Service Providers

Source: OIG-created summary of threat information sources.

EVALUATION RESULTS

The FDIC has implemented processes for the sharing of threat and vulnerability information with financial institutions. For example, the FDIC established formal procedures to communicate cyber threat and vulnerability information. However, the FDIC can improve the effectiveness of its processes to ensure financial institutions receive actionable and relevant threat and vulnerability information. We determined that:

- The FDIC can improve its sharing of threat and vulnerability information with financial institutions or other financial sector entities;
- The FDIC can improve its controls over the recording of computer-security incidents reported by banks and service providers to support threat intelligence operations and sharing activities;
- The FDIC can mature its threat information sharing program by establishing procedures for sharing non-cyber related threat information and revising the program's existing policies and procedures; and
- The FDIC can enhance capabilities to identify threat and vulnerability information.

With these improvements, the FDIC will be better positioned to share accurate, complete, and relevant threat and vulnerability information with financial institutions.

The FDIC, as a member of the FFIEC, has jointly stated that financial institutions should have an effective threat intelligence program, including methods for gathering, monitoring, sharing, and responding to threat and vulnerability information, which supports banks' safety and soundness. FDIC officials stated that other U.S. government and private sector entities are proficient at providing threat information to banks. As a result, FDIC officials stated that the sharing of this same information is unnecessary. However, Congress created the FDIC to maintain stability and public confidence in the Nation's financial system. Sharing relevant FDIC generated threat and vulnerability information with financial institutions or other financial sector entities helps to meet this mission. Specifically, information sharing improves financial institutions' ability to detect, respond, assess, and focus on threats and vulnerabilities relevant to their operations.

The FDIC Can Improve Its Sharing of Threat and Vulnerability Information with Financial Institutions and Other Financial Sector Entities

Historically, the FDIC's Division of Risk Management Supervision (RMS) has shared relevant cyber threat and vulnerability information with financial institutions prepared by other sources, such as the DHS CISA, the Treasury Department, and the FBI. RMS has also engaged in targeted communications during Zero-Day vulnerability attacks.[17] However, RMS has not shared other internally generated threat and vulnerability information gathered from its supervision activities with all financial institutions and other financial sector entities.

According to the National Institute of Standards and Technology (NIST) Special Publication 800-150 Guide to Cyber Threat Information Sharing, by exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. In addition, the 2013 National Infrastructure Protection Plan (NIPP), issued by the DHS, highlights the need to share accurate information and analysis on current and future risks to strengthen and secure the critical infrastructure. It emphasizes that the public-private partnership is central to maintaining critical infrastructure security and resilience.

The U.S. Departments of Treasury and Homeland Security, in coordination with Financial Sector Councils and Committees,[18] developed the Financial Services Sector-Specific Plan (Sector-Specific Plan) in 2015. According to the Sector-Specific Plan, the security and resilience of the Financial Services Sector depends on close collaboration among a broad set of partners, including Financial Services Sector companies; sector trade associations; Federal government agencies; financial regulators; State, local, tribal, and territorial governments; and other government and private-sector partners in the U.S. and around the world. The Sector-Specific Plan emphasizes that sharing timely and actionable information among all of the partners is critical to managing cybersecurity and physical risk. According to the Sector-Specific Plan, the partners share information from government to the sector, from the sector to government, between institutions, across other sectors, and with international partners via an expanding and increasingly effective framework of information sharing mechanisms.

[17] The National Institute of Standards and Technology (NIST) defines a zero-day attack as an attack that exploits a previously unknown hardware, firmware, or software vulnerability. See NIST Interagency Report 8011 Vol. 3, *Automation Support for Security Control Assessments Software Asset Management* (December 2018).
[18] This includes the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the FBIIC.

As detailed below, we identified three examples of unique threat and vulnerability information maintained by and communicated internally within the FDIC that could be helpful to financial institutions or their significant service providers (SSP),[19] but was not shared with them.

(1) 2022 Ransomware Horizontal Review[20] – RMS performed this horizontal analysis on ransomware incidents occurring at FDIC-supervised banks. The review identified the attack vectors used,[21] the ransomware variants,[22] and the top controls in place to mitigate vulnerabilities and prevent such attacks. RMS communicated a summary of the results of its 2022 Ransomware Horizontal Review in various forums throughout 2022 and 2023. Included in these forums were the Community Bankers Symposium in Chicago, a joint FBIIC / FSSCC meeting, and two separate meetings of the Advisory Committee on Community Banking.[23] However, RMS has not formally shared the results of this review more broadly with financial institutions or published the final 2022 Ransomware Horizontal Review since it was completed in December 2022.

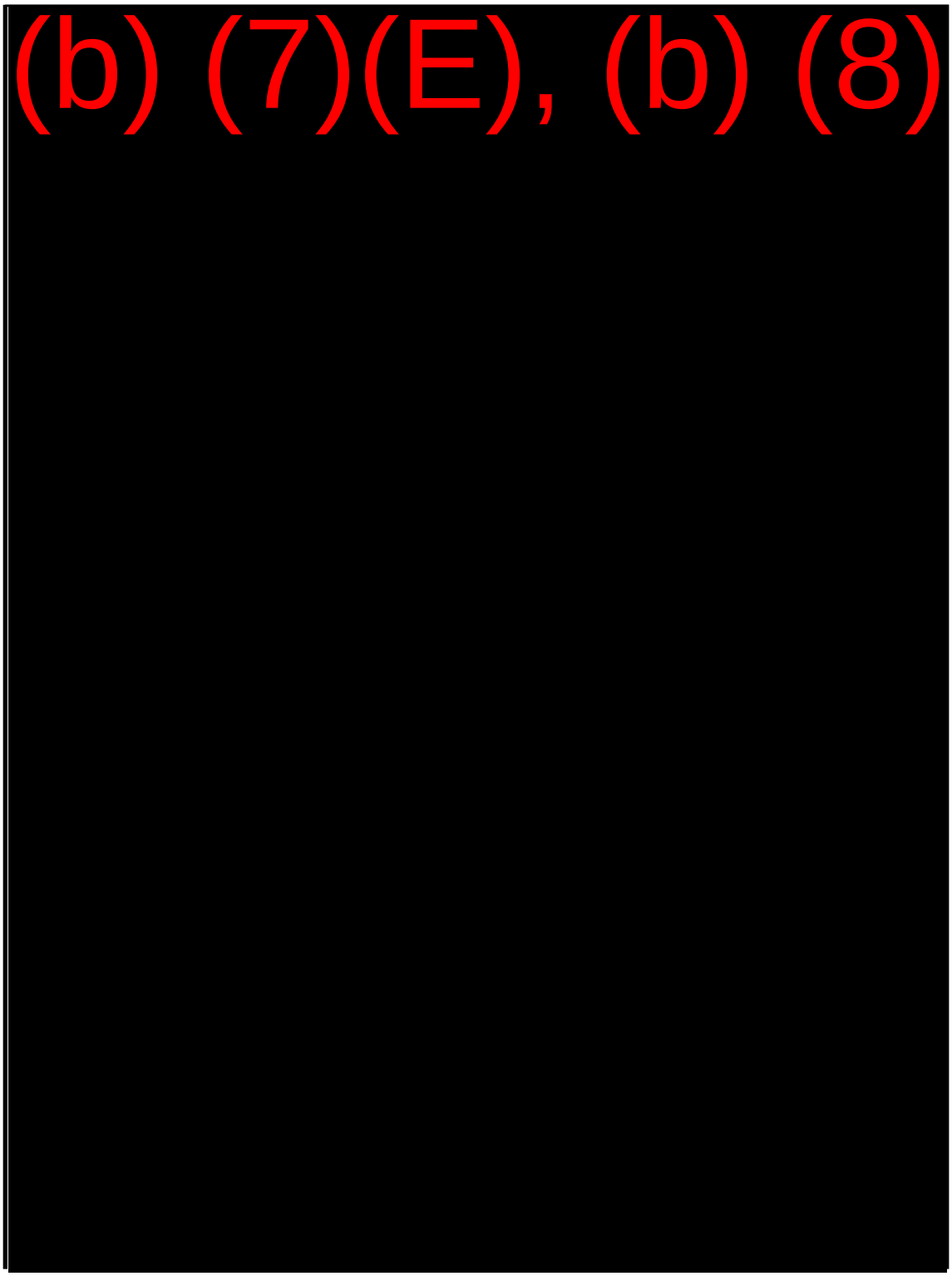
(2) (b) (7)(E), (b) (8) – RMS conducts analysis on its examination and other internal data and compiles a (b) (7)(E), (b) (8) for its examiners for consideration during their ongoing bank examination activities. The RMS (b) (7)(E), (b) (8) includes relevant information on threat and vulnerability trends identified from FDIC bank supervision activities. Specific examples of relevant threat and vulnerability trend information that we identified in the RMS-developed (b) (7)(E), (b) (8) which may be helpful to financial institutions include: (1) trends on security incidents at FDIC-supervised banks (summarized by bank asset size and incident category) and (2) trend analysis on Suspicious Activity Report (SAR) filings by FDIC-supervised financial institutions (summarized by suspicious activity type). Examples of this information as it appears in the RMS (b) (7)(E), (b) (8) are provided in Figure 1.

[19] SSPs can be defined as large and complex service providers designated for special monitoring and collaborative interagency supervision at the national level. SSPs typically provide services through a number of technology service centers in multiple geographic regions. The FDIC and its financial regulatory partners examine SSPs jointly on an annual basis.
[20] The *Ransomware Horizontal: 2022* defines ransomware as a type of malware designed to encrypt files on a device rendering the files unreadable. Malicious actors then demand ransom in exchange for decryption.
[21] An attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Common cyberattack vectors include viruses and malware, email attachments, webpages, pop-up windows, instant messages, chatrooms, and deception.
[22] A variant refers to the type of Malware.
[23] The summary results presented at the Advisory Committee on Community Banking are available on FDIC.gov.

(3) (b) (7)(E), (b) (8) [redacted]

[redacted]

Figure 1: Unique Threat and Vulnerability Trend Information in the FDIC's (b) (7)(E), (b) (8)



Source: RMS (b) (7)(E), (b) (8) (December 2022).

As part our evaluation we coordinated with banking associations to issue a survey to their member financial institutions on their threat intelligence operations and needs. Based on this survey, 79 percent of respondents identified the FDIC as a source of threat and vulnerability information for their operations.[26] As summarized in Table 2 below, banks responded that the threat information received from the FDIC was actionable, relevant, and provided moderate to high[27] value to their operations.

Table 2: FDIC Threat Information Survey Results

Threat Information Received From the FDIC…	Result (% in agreement)
Is Actionable	**85%**
Is Relevant	**86%**
Provides Moderate to High Value	**78%**

Source: OIG survey results from financial institutions receiving threat and vulnerability information.

The surveyed financial institutions identified that the top threats to their operations were those related to (1) Information Technology (IT) and cyber and (2) fraud.[28] Half of the survey respondents also indicated that the threat information received from the FDIC was given additional consideration. In addition, certain financial institutions indicated that information from the FDIC was taken more seriously within their organizations than that received from other sources. They also stated that FDIC-provided threat information was given more emphasis and support from higher levels of bank management than that received from other sources.

Financial institutions responding to our survey also specifically noted that their threat intelligence programs would benefit from the following information from the FDIC:

(1) Benchmarking of threat information across the sector;
(2) Deeper insight into successful mitigations against attacks; and
(3) Industry-specific data and trending.

Representatives from three banking associations we interviewed also stated that the FDIC could provide added value to banks and their threat intelligence programs by sharing trend analysis of examination data and bank-reported cybersecurity incidents.

[26] Twenty-four banks responded to this specific survey question. Nineteen of the 24 respondents (79 percent), identified the FDIC as a source of threat and vulnerability information.
[27] Critical to financial institution decision making.
[28] See Table 3 of this report for further details.

Overall, this feedback demonstrates the interest and need financial institutions have for the FDIC developed IT and Bank Secrecy Act / Anti-Money Laundering (BSA/AML) threat trends and other information that the FDIC maintains and communicates internally.

We note that the FDIC provides Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT)[29] resources and information on the Banker Resource Center of the FDIC's public website. This information includes National Strategies and Risk Assessments created by the Treasury Department and Financial Institution Letters (FIL) jointly issued by the Federal Regulators. However, this information on AML/CFT could be expanded to include other FinCEN related reports and FDIC generated products.

According to RMS officials, financial institutions have the responsibility to gather and receive threat and vulnerability information to demonstrate their implementation of effective threat intelligence programs. RMS officials stated that the FDIC evaluates the adequacy of bank threat intelligence programs during its IT examinations when assessing the overall safety and soundness of financial institutions. Specifically, as part of the FDIC's Information Technology Risk Examination (InTREx) program, examiners evaluate the financial institution's IT risk assessment process. Pursuant to the InTREx program, examiners are instructed to consider whether an institution belongs or subscribes to appropriate threat and vulnerability information-sharing sources and whether the threat information used to monitor threats and vulnerabilities is adequate given the institution's complexity. According to an RMS official, if a bank does not have an adequate threat intelligence program, it would be identified as a deficiency and addressed within the FDIC's Report of Examination (ROE). As of March 2023, RMS reported that based on the most current ROEs, five of approximately 3,000 FDIC-regulated banks were determined to have weak threat intelligence programs.

RMS officials also emphasized that on multiple occasions the FDIC has jointly coordinated with other FFIEC members, to communicate to banks the importance of receiving adequate threat information and has encouraged banks to join threat intelligence sharing groups, such as the FS-ISAC.[30] However, according to statistics shared with the FDIC during our evaluation, over one-third of FDIC-insured institutions were not members of FS-ISAC.[31]

[29] The Anti-Money Laundering Act of 2020 (AML Act) modified part of the BSA and requires financial institutions to have reasonably designed risk-based programs to prevent money laundering and the financing of terrorism. By statute, individuals, banks, and other financial institutions are subject to the BSA recordkeeping requirements. For purposes of consistency with the AML Act, the FDIC now uses the term "AML/CFT" rather than "BSA/AML".
[30] 2014 FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement.
[31] Banks may receive threat intelligence information from other subscription-based service vendors.

As highlighted in this report, there are many sources of threat information for financial institutions. For example, the FinCEN publishes summary information from the SAR data it collects.[32] This open source data can be filtered and searched by suspicious activity type and narrowed down by a financial regulator to create analyses similar to those that RMS is producing for its (b) (7)(E), (b) (8) and examination staff. RMS officials have also promoted other Federal sources of threat information to banks, such as CISA.[33] This includes highlighting CISA's www.StopRansomware.gov site as a key source for ransomware information for financial institutions. However, while this CISA site contains ransomware information, including vectors and prevention and detection controls, it does not contain the information on ransomware events experienced by FDIC-supervised institutions like that presented in the 2022 Ransomware Horizontal Review. For example, the 2022 Ransomware Horizontal Review includes the number of ransomware incidents at FDIC-supervised institutions occurring between June 2019 and May 2021, and details the number of incidents that affected the institutions directly versus those impacting a bank through a service provider connection. The 2022 Ransomware Horizontal Review also details the impact severity,[34] associated ransomware payments, and provides information on the specific ransomware attack vectors and variants. This FDIC unique threat and vulnerability information product could provide FDIC-supervised financial institutions with accessible and specific threat and vulnerability information for consideration within their operations. Additionally, this report would help reduce administrative burden on financial institutions that would otherwise have to independently perform research on these publicly available sites to gather ransomware threat and vulnerability information.

RMS officials acknowledged that the 2022 Ransomware Horizontal Review would be helpful and relevant for banks and have already communicated the information in various forums, including with financial institutions at the 16th annual Community Bankers Symposium in Chicago. RMS officials noted that they are working to share the results of the 2022 Ransomware Horizontal Review more broadly with financial institutions. RMS officials acknowledged that the other examples that we identified above constitute threat and vulnerability information. However, they questioned the uniqueness and usefulness of some of this information for banks. Specifically, RMS officials explained that they did not believe that providing computer-security incidents by bank size or type would be overly helpful to banks. In addition, RMS officials cited FinCEN as the authoritative source for trends on SARs. Further, as detailed later in this report, the RMS Threat Communication Operating Procedures were intended to be applied only to cyber threat and vulnerability information. Therefore, the procedures would not facilitate the sharing of any non-cyber related threat information.

[32] See FinCEN.gov public website for more information.
[33] FIL-50-2022: Updated FFIEC Cybersecurity Resource Guide for Financial Institutions (October 27, 2022).
[34] Based on the 2022 Ransomware Horizontal Review, the FDIC developed a simple incident impact calculus with corresponding severity ratings - High, Moderate, and Low.

Based on the results of our survey, approximately 60 percent of banks stated that while the information from the FDIC was repetitive of information received from other vendors, it was still beneficial. In addition, according to our interviews with FS-ISAC officials and banking associations, this type of information is beneficial to banks because it ultimately reaches the attention of bank executives, rather than just the bank's IT group.

RMS officials stated that they carefully select the information they choose to share externally based on several criteria, including whether the information has already been shared by other entities and whether the information is actionable. RMS officials stated that this helps ensure that banks give FDIC threat and vulnerability communications the proper attention. RMS officials expressed concern that banks may divert attention away from the threat information that is most relevant to their unique characteristics just because they receive other threat information from the regulator. RMS officials also indicated that banks may be motivated to focus on FDIC-issued information to prepare for examinations and avoid examiner criticism. RMS officials asserted that banks should be focused on good IT risk management rather than a clean ROE.

We disagree with RMS's position and believe that regardless of the motivation by the bank, threat information issued by the FDIC is beneficial. Further, we believe FDIC-supervised institutions, and more broadly, FDIC-insured institutions could benefit from receiving unique threat and vulnerability information generated by the FDIC and threat and vulnerability trending analyses that the FDIC has developed. RMS's concerns that increasing the amount of threat information sent to financial institutions may desensitize the banks to FDIC communications is also not supported by the Federal Government's Financial Services Sector-Specific Plan. As noted above, the Sector-Specific Plan states that the security and resilience of the Financial Services Sector depends on close collaboration among a broad set of partners, including Financial Services Sector companies; sector trade associations; Federal government agencies; financial regulators; State, local, tribal, and territorial governments; and other government and private-sector partners in the U.S. and around the world. The Sector-Specific Plan emphasizes that sharing timely and actionable information among all of the partners is critical to managing cybersecurity and physical risk. According to the Sector-Specific Plan, the partners share information from government to the sector, from the sector to government, between institutions, across other sectors, and with international partners via an expanding and increasingly effective framework of information sharing mechanisms.

By sharing relevant threat and vulnerability information with banks, the FDIC could improve the ability of financial institutions to detect, respond, assess, or focus on threats and vulnerabilities relevant to their operations. Threat and vulnerability

information that is uniquely developed or summarized by the FDIC, such as trends identified from SAR filings specific to FDIC-supervised banks, could inform key officials at banks, including the BSA/AML Officer or Chief Audit Executive, of relevant threats for fraudulent activity. This information could help banks focus resources and ensure adequate controls are in place for high-trending fraud areas, which in turn, could help mitigate the banks' susceptibility to such threats. Similarly, uniquely summarized trends on IT security incidents reported by FDIC-regulated banks can inform bank Chief Information Officers or Chief Information Security Officers of relevant cyber threats to banks. Such information could help banks focus resources to ensure adequate controls are in place for trending security incidents, helping to mitigate the banks susceptibility to such threats. Through the increased sharing of uniquely developed or summarized threat and vulnerability information by the FDIC, banks can be better equipped to identify and address key weaknesses that threat actors could exploit, improve controls, or confirm the areas of focus for their risk assessment and threat intelligence efforts.

Recommendation

We recommend the FDIC Director of RMS:

1. Share threat and vulnerability information that is uniquely developed or summarized by the FDIC with financial institutions or other financial sector entities to further strengthen their threat intelligence activities. This includes results from the FDIC's 2022 Ransomware Horizontal Review and relevant trending and analysis conducted by the Division of Risk Management Supervision.

The FDIC Can Improve Its Controls over the Recording of Computer-Security Incidents to Support FDIC Threat Intelligence Operations and Sharing Activities

The RMS Regional Computer-Security Incident Response Guide (RCIRG) requires RMS examination staff to record all computer-security incidents reported by financial institutions or service providers to the FDIC in the Virtual Supervisory Information on the Net (ViSION) system. However, we determined that the FDIC's controls were not effective to ensure it maintains complete and accurate data in ViSION on all computer-security incidents reported by banks and service providers.

> *A computer-security incident is an occurrence that jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits. A computer-security incident may be caused by either human action or a natural phenomenon.*
>
> **The RMS Regional Computer-Security Incident Response Guide (RCIRG)**

Improved Controls over Computer-Security Incidents

A 2021 RMS internal review of nine bank-reported computer-security incidents in the FDIC's Atlanta Region found that four of the nine incidents (44 percent) did not have an associated ViSION incident report.[35] Further, a 2022 RMS internal review of 13 bank-reported computer-security incidents in the FDIC's Dallas Region found that 2 of the 13 incidents (15 percent) did not have a ViSION incident report.[36] RMS officials stated that these omissions were discussed with the Regions and that corrective actions were taken. ViSION records were subsequently created for missing incidents, as appropriate. In response to the identified weaknesses, RMS issued supplemental guidance in October 2022 to help ensure examiners capture all computer-security incidents in ViSION. Details on the supplemental guidance are provided in Figure 2.

[35] According to RMS officials, the Atlanta Region was not reporting incidents they did not consider significant.
[36] According to RMS officials, the Dallas Region interpreted FDIC guidance at the time that incidents occurring at banks, but stemming from a service provider, would be recorded under the service provider, not the bank individually.

Figure 2: ViSION Supplemental Guidance Documents

- **Incident Patterns and Definitions** - provides the definitions of incidents (detailed below). The document also provides information on selecting more than one "nature of incident" in ViSION in cases where the report includes multiple incident types.
- **Incident Reporting Decisions** - provides users with guidance on how to determine when to add a computer-security incident record in ViSION.
- **ViSION Security Incident Comments Format and Content** - provides guidance on specific information that should be collected for all security incidents, including an overview of the incident; corrective actions; the methods, procedures, and tools used; impact and severity level; and recovery actions.

Source: RMS supplemental guidance provided to examiners for incident entry in ViSION.

The supplemental guidance also included a definition for "critical" incident and defined the various incident patterns as presented in Figure 3.

> *A "critical" incident is that which disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the banking organization's operations, result in customers being unable to access their deposit and other accounts, or may affect the stability of the financial sector. This may include major computer-system failure; cyber-related interruption, such as a distributed denial of service or ransomware attack; or another type of significant operational interruption.*
>
> **RMS Supplemental Guidance -**
> ***Incident Reporting Decisions***

Figure 3: Incident Patterns and Definitions

- **Crimeware** - Any incident involving malware[37] designed to carry out or facilitate illegal online activity that is usually financially motivated. Ransomware is an example of Crimeware.
- **Debit/Credit Card Breach** - Data breaches that involve the compromise of Credit or Debit card data only.
- **Denial-of-Service Attacks** - Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.
- **Electronic Funds Transfer Fraud** - Any attack in which Automated Clearing House or wire transfer systems are targeted for financial gain.
- **Insider or Privilege Misuse** - All incidents involving any unapproved or malicious use of organizational resources fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (those granted privileges) apply.
- **Miscellaneous Errors** - Incidents where unintentional actions directly compromised a security attribute of an information asset.
- **Payment Card Skimmers** - All incidents in which a skimming device is physically implanted on an Automated Teller Machine that reads magnetic stripe data from a payment card.
- **Phishing Attacks/Social Engineering** - Data breach or system compromise that involve the breach of networks and systems and/or result in a degradation or interruption of service as a result of a targeted phishing or social engineering incident.
- **Physical Theft and Loss** - Any incident where a physical information-related asset went missing, whether through misplacement or malice.
- **Supply Chain Compromise** - A hardware or software vulnerability, prior to or as part of an update to systems, software, or application development tools acquired by an end user (e.g., SolarWinds incident).
- **Web Application Attacks** - Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.

Source: RMS supplemental guidance provided to examiners for incident entry in ViSION.

[37] Malware is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

The FDIC has recognized the need to improve the quality of the incident data in ViSION and for issuing supplemental guidance to FDIC Regions. Specifically, the supplemental guidance provided examiners with instructions that will help ensure computer-security incidents are properly and consistently categorized by type and appropriately marked as critical versus non-critical incidents. Further, the supplemental guidance defined what specific information should be collected consistently for all security incidents. An RMS official also explained that marking events as "critical" is important so that the FDIC can prepare for the bank's operational failure, should it occur. The official added that the more time the FDIC has, the better prepared it will be. While this guidance should help ensure future information is recorded consistently and accurately, historical data may need further review and correction.

For example, the 2021 review of the Atlanta Regional Office determined that seven of nine incidents did not have an incident severity rating level. In reviewing FDIC computer security incident response information, we identified a reported incident where (1) a bank's systems were compromised, but were fully recovered within a week, (2) a ransom was paid to the threat actor to ensure the compromised data was not published, and (3) the bank had to rebuild its network.[38] However, the incident was not marked as "critical" within the ViSION record.

We identified a similar incident at a service provider where (1) a ransom was paid and (2) the incident impacted 18 financial institutions that had their customers data breached.[39] This incident was also not marked "critical" within the ViSION record.[40] For other incidents, the recorded comments indicated that the incidents should have been labeled as "Crimeware" as they involved financially motivated ransomware attacks. However, these crimeware incidents were labeled by FDIC examiners as either "Insider or Privilege Misuse", "Web Application Attack", or "Denial of Service Attack."[41] These incident patterns are defined above in Figure 3.

[redacted]

[40] We conducted additional follow-up on incidents that we identified were not marked critical in ViSION but appeared to meet the definition. According to RMS officials, generally, regional staff are "closest" to the incident and use their best judgement when determining the criticality. In the specific examples we identified, RMS officials relied on the Regions' judgement and did not indicate whether the criticality decision was or was not correct. In both of the examples provided, while we disagree with the criticality determination based on the definition of critical, RMS Incident Reports were created and, therefore, the RMS Washington Office was notified of the incident.

[41] We conducted additional follow-up on several incidents that we identified in ViSION where, based on the FDIC's definitions of the incident categories, the selected category in ViSION did not seem most appropriate. According to RMS officials, the broad generalization of incident categories is to avoid listing every conceivable incident type. RMS stated that regional staff have discretion and use their judgement to categorize an incident as best possible. For the examples we identified, RMS explained that while the incident at the service provider was ransomware, the ransomware did not spread to the bank, and therefore the regions did not categorize the incident as "Crimeware", but rather categorized it based on how it impacted the bank.

According to RMS officials, the data inaccuracies and inconsistencies we observed could have occurred because of the discretion exercised by the FDIC Regions when determining whether to add a ViSION record and what information to include. For example, an RMS official explained that if the incident has already been resolved by the bank with low impact, there may be discretion exercised by examination staff to not record the event in ViSION. RMS officials also explained that, in the past and prior to the development of improved instructions, lower level incidents would not have been recorded in ViSION, but would possibly be recorded in the Regional Automated Document Distribution system.[42] RMS officials also indicated that data inaccuracies could have occurred due to examination staff receiving the incident information from banks but forgetting the Regional Directors (RD) memorandum instructions.[43] RMS officials added that it could also be that examination staff did not understand the changes associated with the new rule. The FDIC agreed that regardless, the data should be accurate.

Improved Controls over Severe Incidents

Given the identified examples over the inaccuracy and incompleteness of computer-security incidents recorded in ViSION, we believe the FDIC could further improve its controls over recording the most severe incidents, including the incidents banks are required to report under 12 Code of Federal Regulations, Part 304: *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Notification Rule).[44]

[42] See Appendix 3 for the entire Severity Schema from the RCIRG, which describes the timing to which reporting should occur based on the severity of the incident.
[43] RMS RD Memorandum 2022-021 *Computer Security Incident Response Procedures, August 12*, 2022.
[44] Final Rule, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

The FDIC, along with other Federal banking regulators, issued the Notification Rule requiring banks to notify the FDIC about certain computer-security incidents within 36 hours of the event. The Notification Rule became effective on May 1, 2022.

A "notification incident" is defined as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability 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; (ii) business line(s), including associated operations, services, functions and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, 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

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Notification Rule)

According to the Notification Rule, banks must inform their primary bank regulator when a computer-security incident materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's ability to carry out its banking operations, the bank's business lines, or associated operations. To implement the Notification Rule, the FDIC issued a FIL on March 29, 2022 explaining that FDIC-supervised banks can comply with the rule by:

(1) Reporting an incident to their case manager;[45]
(2) Reporting an incident to an examination team if the event occurs during an examination; or
(3) In the event that the bank is unable to access its supervisory team contacts, the bank may notify the FDIC at a designated email address established specifically for reporting such incidents.

According to RMS officials, when the FDIC jointly developed the Notification Rule, RMS was intentional in its efforts not to increase the regulatory burden on financial institutions by requiring formal reporting of notification incidents. By giving the banks increased flexibility on the avenues to report such incidents, the FDIC hoped it would facilitate the prompt reporting of all events in accordance with the Notification Rule and other rules. However, in light of the computer-security incident reporting documentation issues previously discussed, including the discretion exercised by the

[45] According to the RMS Case Manager Procedures, an FDIC case manager, in conjunction with senior management, coordinates and directs the supervisory program using a top-down approach to develop strategies and examination activities for all insured depository institutions in their caseload. The primary responsibilities of FDIC case managers involve assessing risk to the Deposit Insurance Fund and directing the appropriate supervisory efforts to eliminate or manage such risk.

FDIC Regions, computer-security incident information related to the most severe incidents may not be properly recorded in ViSION.

According to RMS officials, however, they do not rely on ViSION data as the primary source for research and analysis on computer-security incidents, including the most severe incidents - those with a severity level 3, 4, or 5.[46] Instead, RMS officials indicated they rely on RMS Incident Reports that FDIC Regional Office personnel are required to complete for reported incidents categorized as severity level 2 and above.[47] According to RMS officials, the RMS Incident Reports are stored on an internal shared site, accessible only by those with a legitimate business need for the incident details. The RMS Incident Reports include important information about the financial institution, incident date, points of contact, and details on the incident. Further, the Incident Reports include the designated severity level, which would allow RMS to identify, track, and trend the most severe incidents.

Nevertheless, as discussed above, an RMS internal review found that RMS Incident Reports did not always include the designated severity level. In addition, we reviewed computer security incidents reported to the FDIC between January 1, 2019 and October 31, 2022 and assessed the supporting RMS Incident Reports for select cases. We found that the designated severity levels presented in the RMS Incident Reports did not always appear appropriate given the details associated to the incidents. For example, in one reported incident, a bank's systems were compromised, but were fully recovered within a week; a ransom was paid to the threat actor to ensure the compromised data was not published; and the bank had to rebuild its network.[48] According to the RMS Incident Report, the FDIC designated the incident as severity level 1.[49] In another reported incident at a Service Provider, a ransom was paid and 18 financial institutions had their customers data breached.[50] According to this RMS Incident Report, the FDIC designated the incident as severity level 1.

Given the multiple avenues provided to banks to facilitate their prompt reporting of all events in accordance with the Notification Rule and other rules, it is critical that controls over RMS Incident Reports and ViSION ensure accurate and complete information. Inaccurate and incomplete incident information may limit the FDIC's

[46] See Appendix 3 for the RMS RCIRG Severity Schema.
[47] According to the RCIRG, RMS Regional Office personnel must record all computer-security incidents reported to the FDIC in ViSION. For those incidents categorized as severity level 2 and above, FDIC officials must also create an RMS Incident Report. See Appendix 3 for a listing of severity levels. The RCIRG also instructs RMS employees to update the ViSION record and the RMS Incident Report as new information is gathered.
[48] (b) (7)(E), (b) (8)
[49] The RCIRG defines a severity level 1 incident as an incident unlikely to impact financial services operations of insured depository institutions or service providers and indicates localized, contained compromise or disruption of an insured depository institution. Further, according to the RCIRG for severity level 1 incidents, either no exploits have been identified or the exploits resulted in no significant damage, disruption, or system compromise. See Appendix 3 for more information.
[50] (b) (7)(E), (b) (8)

ability to conduct critical research and trend analyses on threats and vulnerabilities and impede its ability to share accurate, complete, and relevant information internally with its examination staff and externally with financial institutions.

Recent events in the financial sector have highlighted the expediency in which the viability of a bank can be impacted when depositors lose confidence in management's ability to operate the bank in a safe and sound manner. As seen with Silicon Valley Bank and Signature Bank, a lack of depositor confidence can lead to failure and a significant impact to consumers and the Deposit Insurance Fund. While a bank failure caused by a computer-security incident has yet to be realized,[51] the threat posed by both malicious actors and ransomware is real. According to the Federal Reserve Board, cybersecurity risks may affect financial stability because traditional stabilizing responses (capital and liquidity) are not likely to resolve such an attack. Further, the Federal Reserve Board noted that interconnected payment and settlement systems make it difficult to restore operations after a cybersecurity incident and as a result, "[u]ncertainty about the nature and extent of an incident may prompt runs on [the bank's] counterparties, competitors, or unaffected segments of the firm's operations." These experiences emphasize the need to ensure that complete and accurate information is shared with the appropriate officials in a timely manner.

Recommendations

We recommend the FDIC Director of RMS:

2. Conduct training for examiners on the requirements for recording computer-security incidents, the information to include, and specific requirements for Notification Rule incidents.

3. Improve controls over the intake and recording of computer-security incidents reported by banks and service providers to ensure that: (1) records are added to the Virtual Supervisory Information on the Net system as required, (2) recorded incident information in the Virtual Supervisory Information on the Net system and in the Division of Risk Management Supervision Incident Reports is complete, appropriate, and accurate, and (3) the most severe incidents can be readily identified to promote early awareness of emerging threats.

4. Conduct a review of computer-security incidents reported since May 1, 2022 to ensure Virtual Supervisory Information on the Net system records are complete and accurate.

[51] We reviewed reports on failed banks for the period January 1, 2019 through November 30, 2022.

Maturing the FDIC's Threat Information Sharing Program

The FDIC established the Intelligence and Threat Sharing Unit (ITSU) to centralize its intelligence functions and coordinate a network of liaisons from key FDIC Divisions and Offices to "increase the communities of practice associated with threat information analysis and dissemination across the FDIC."[52] The FDIC chartered the FDIC's Intelligence Support Program (ISP), to coordinate FDIC threat information acquisition, analysis, and production. The RMS Operational Risk group identifies, monitors, and analyzes information about operational risks that can threaten the safety and soundness of FDIC-supervised financial institutions. As such, the FDIC has traditionally relied on RMS's Operational Risk group to communicate cyber-related threat information internally to examiners and externally to financial institutions. We identified three key areas that the FDIC can emphasize as it works to further mature its threat information sharing program. This includes: (1) establishing procedures for the sharing of non-cyber threat information, (2) improving FDIC existing threat sharing procedures, and (3) developing performance measures to assess the effectiveness of external threat sharing activities.

The FDIC Needs to Establish Procedures for Sharing Non-Cyber Threat Information

The U.S. Government Accountability Office (GAO) Internal Control Standards[53] state that internal control comprises the plans, methods, policies, and procedures used to fulfill the mission and objectives of the organization. Management is responsible for designing policies and procedures that support the organization's operations. In January 2022, we reported that the FDIC had not established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions.[54] Our report contained 25 recommendations to improve the FDIC's threat sharing operations. Specifically, we recommended that the RMS Director establish and implement procedures for RMS threat information sharing activities. In response to this recommendation, in July 2022, RMS implemented the RMS Threat and Vulnerability Communication Operating Procedures (RMS Threat Communication Operating Procedures).

The RMS Threat Communication Operating Procedures formalize the FDIC's methods for communicating threat and vulnerability information internally with examination staff and externally with financial institutions. However, according to

[52] FDIC Management Response to OIG Draft Audit Report, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (November 5, 2021).
[53] GAO's *Standards for Internal Control in the Federal Government* (September 2014) (Internal Control Standards).
[54] FDIC OIG, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (AUD-22-003) (January 2022).

RMS officials, these procedures were only intended for the sharing of cyber or computer-security related threat and vulnerability information. As a result, the FDIC needs to establish procedures for the external sharing of unclassified non-cyber threat information that it may obtain or develop internally.

The FDIC's Charter for the ISP states that the Division of Administration's (DOA) ISP is responsible for coordinating threat information acquisition, analysis, and production and that DOA designed the ISP to augment the existing threat information acquisition, analysis, and production processes in FDIC Divisions and Offices. According to the ISP Charter, the ISP is responsible for identifying Division and Office threat information needs, identifying relevant threat information databases and sources, and sharing DOA ITSU-authored and other agency-authored intelligence products[55] aligned to the FDIC's threat information needs. The ISP Charter further states that Division and Office subject matter experts shall:

- Provide program outputs to respective Division and Office stakeholders;
- Champion new ISP initiatives within their Divisions and Offices and any related threat information sharing; and
- Provide Division or Office, and other agency points of contact with whom to appropriately share and receive threat information.

The FDIC's ITSU focuses on a broader all-hazards approach to threat information sharing.[56]

In addition, the interagency paper entitled Sound Practices to Strengthen Operational Resilience[57] (Sound Practices Paper) jointly issued in October 2020 by the FDIC with the Federal Reserve Board and the Office of the Controller of Currency supports an all-hazards approach to threat intelligence. The Sound Practices Paper provides firms with ways to strengthen their operational resilience in the face of internal and external operational risks that, left unchecked, could lead to wide-scale disruption.

The Sound Practices Paper states:

> *In recent years, firms have experienced significant challenges from a wide range of disruptive events including technology-based failures, cyber incidents, pandemic outbreaks, and natural disasters. While advances in technology have improved firms' ability to identify and recover from various types of disruptions,*

[55] In accordance with FDIC Directive 1350.04 Document Labeling, all ITSU-authored threat products that contain controlled sensitive information must be properly designated and disseminated in accordance with the FDIC Document Labeling Framework that prohibits controlled information from being released publicly.
[56] FDIC Directive 1600.09, provides policy, assigns responsibilities, and prescribes processes for the acquisition, analysis, production, and dissemination of **"all-hazard threat information"** under the FDIC ISP. **All-hazard threat information** is defined as, "Comprehensive data of threats, including (but not limited to): foreign intelligence entities, terrorists, criminals, natural disasters, cyber-enabled threats, and insider risks."
[57] FIL-103-2020: Sound Practices to Strengthen Operational Resilience (November 2, 2020).

increasingly sophisticated cyber threats and growing reliance on third parties continue to expose firms to a range of operational risks.

The Sound Practices Paper further defines Operational Resilience as the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard.

During this evaluation, FDIC officials explained that the Threat Communication Operating Procedures were only intended to focus on and apply to cyber and computer-security related threats and vulnerabilities. FDIC officials explained that RMS was unlikely to uniquely obtain, or be in a position to uniquely share, other threat information types –such as physical threats, environmental threats, and fraud related threats - with financial institutions. However, this focus may limit the FDIC's ability to effectively communicate other relevant threat and vulnerability information with financial institutions in a timely manner. For example, as previously noted in this report, RMS develops unique trending on non-cyber related SAR information for its examination staff that could benefit banks.[58] In addition, according to FDIC officials, the FDIC could receive physical threat information related to banks or banking officials that could be shared with financial institutions. Further, the FDIC's standing information needs[59] supports that ITSU may develop non-cyber related threat intelligence products that could be relevant to financial institutions. This includes intelligence products focused on:

- Domestic Violent Extremist or Criminal Threats;
- Foreign Intelligence Entities' Targeting Insured Financial Institutions and Bank Service Providers;
- Adversarial Nation-State Actors Targeting Insured Financial Institutions, and Bank Service Providers;
- Threats from Criminal Actors Engaging in Money Laundering through Insured Financial Institutions;
- Terrorist Targeting or Financing through the U.S. Financial Sector, Insured Financial Institutions, and Bank Service Providers;
- Threats to U.S. Tri-Sector Critical Infrastructure (Financial, Energy, & Telecommunications) Partnership Interests; and
- Threats to U.S. Critical Infrastructure in the National Capitol Region, Regional and Field Office Locations, Banking Centers, and Key Service Provider Locations.

[58] FinCEN maintains publicly available information on the SAR data it collects. FinCEN's open source data can be filtered and searched by suspicious activity type and narrowed down by a financial regulator to create analyses similar to those that RMS is producing for its (b) (7)(E), (b) (8) and examination staff. However, this SAR trending related to FDIC-supervised financial institutions generated by the FDIC would be beneficial for banks and help reduce the administrative burden on financial institutions that would otherwise need to independently perform this research.
[59] FDIC ITSU Calendar Year (CY) 2023 Standing Information Needs and Key Intelligence Questions, December 2022.

Under RMS's current Threat Communication Operating Procedures, there is increased risk that such information would not be shared internally with examiners or externally with financial institutions because it may not be cyber-related.

RMS officials explained that the FDIC handles the distribution of other threat information types through alternative channels or procedures, including through regional emergency response procedures for weather-related events and through the FDIC's Consumer News product for communicating consumer fraud-related information. We obtained the Environmental and Natural Disaster Response procedures for the FDIC's Dallas Region. The related external communication responsibilities within these procedures focus on responding to a specific disaster event. However, these procedures do not address the full scope of non-cyber threats to financial institutions as described in this report. In addition, the FDIC Consumer News articles do not communicate targeted fraud against banks.

The FDIC established the ITSU to centralize its intelligence functions and coordinate a network of liaisons from key FDIC Divisions and Offices to increase the communities of practice associated with threat information analysis and dissemination across the FDIC. In turn, the FDIC's RMS Operational Risk group is responsible for identifying, monitoring, and analyzing information about operational risks that can threaten the safety and soundness of FDIC-supervised financial institutions. As such, the RMS Operational Risk group has historically communicated threat information internally to FDIC examiners and externally to financial institutions. Without comprehensive Threat Communication procedures covering all threat types, there is increased risk that RMS may miss opportunities to share unclassified non-cyber related threat information externally or may experience delays in sharing such information. This includes information developed by RMS and unclassified intelligence products developed by the FDIC's Senior Intelligence Officer (SIO). We have no evidence that the FDIC has not shared critical non-cyber threat information with financial institutions. However, without comprehensive procedures, this ultimately increases the risk that non-cyber threat and vulnerability information would not be shared effectively.

Limiting FDIC shared threat information to cyber-related risks also reduces assurance that financial institutions receive relevant threat information they may need. As shown in Table 3, survey responses we received from financial institutions supported that after cybersecurity, fraud was considered the most significant threat to their operations.

Table 3: OIG Survey Results from Financial Institutions - Threat Needs

Threat	% of Respondents
Cyber	**74%**
Fraud	**52%**
Other	**30%**

Source: OIG survey results from financial institutions receiving threat and vulnerability information.

As previously discussed, our interviews with banking associations also supported financial institution interest in financial sector level threat information and relevant threat information developed from FDIC examination activities. This indicates a need for threat information beyond cyber-related instances. Such information may help banks enhance their safety postures and ultimately result in a stronger financial system.

Recommendation

We recommend the Director, RMS, in coordination with ITSU:

5. Ensure FDIC threat and vulnerability communication procedures facilitate the sharing of unclassified non-cyber related threat and vulnerability information.

FDIC Existing Threat Sharing Procedures Need Improvement

The GAO Internal Control Standards state that organizations should document policies that define responsibilities for achieving operational process objectives and addressing related risks. Policies and procedures serve as an important control for making sure 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 make sure employees properly carry out those directives. The Internal Control Standards state that organizations should periodically review their policies and procedures to make sure they are relevant and effective. The National Institute of Standards and Technology (NIST) Special Publication 800-150 Guide to Cyber Threat Information Sharing also states that before sharing threat information, organizations should establish information sharing rules, including the types of threat information that may be shared, the conditions and circumstances when sharing is permitted, and identifying approved recipients.

The RMS Threat Communication Operating Procedures provide a common methodology, including four questions and factors for determining whether a threat[60] or vulnerability[61] should be communicated to FDIC-supervised insured depository institutions, examined service providers, or supervisory personnel. The RMS Threat Communication Operating Procedures also provide information on the delegated authorities for publishing threat and vulnerability information, communication methods, and interagency collaboration. Based on our review of the RMS Threat Communication Operating Procedures and interviews with RMS Operational Risk group officials, we identified four areas for improvement as presented in Figure 4.

Figure 4: Areas for Improvement in RMS Threat Communication Operating Procedures

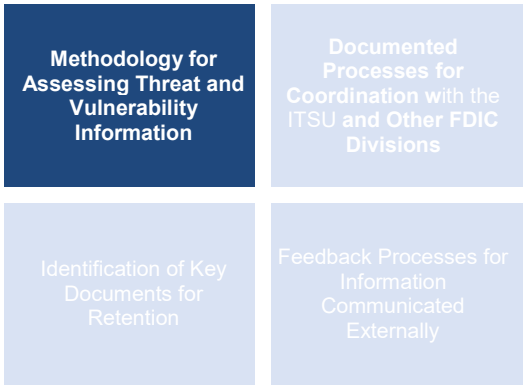
Methodology for Assessing Threat and Vulnerability Information	**Documented Processes for Coordination with the ITSU and Other FDIC Divisions**
Identification of Key Documents for Retention	**Feedback Processes for Information Communicated Externally**

Source: OIG Conclusions based on Evaluation Results.

[60] The RMS Threat Communication Operating Procedures present a definition of threat that is uniquely associated with information systems. Specifically, RMS uses the National Institute of Standards and Technology's (NIST) definition of threat, which is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. NIST Special Publication 800-150 "Guide to Cyber Threat Information Sharing."
[61] The RMS Threat Communication Operating Procedures present a definition of vulnerability that is uniquely associated with information systems. Specifically, RMS uses the National Institute of Standards and Technology's (NIST) definition of vulnerability, which is a weakness in a system, application, or network that is subject to exploitation or misuse. NIST Special Publication 800-61 Rev. 2 "Computer Security Incident Handling Guide."

Methodology for Assessing Threat and Vulnerability Information

Historically, RMS has primarily focused on further disseminating to financial institutions threat and vulnerability information that is created by trusted and reliable sources.[62] The RMS Threat Communication Operating Procedures provide the following four questions for RMS officials to address in determining whether to share threat and vulnerability information:



1. Is the threat or vulnerability credible?
2. Is the information shareable?
3. Does an information gap exist, or is the threat critical enough that a regulatory amplification is warranted?
4. Is the information actionable or is there a "need to know?

For each question, the RMS Threat Communication Operating Procedures provide "Factors to Consider." For question 1, the Factors to Consider include a source reliability rating and methodology. The source reliability rating and methodology uses two variables, source reliability and information accuracy to measure how reliable and accurate any given threat or vulnerability is at a point in time.[63] Table 4 provides information on these two variables.

Table 4: Source Reliability Rating and Methodology

Source Reliability		Information Accuracy	
A	Reliable	**1**	Confirmed
B	Usually Reliable	**2**	Probably True
C	Fairly Reliable	**3**	Possibly True
D	Not Usually Reliable	**4**	Doubtfully True
E	Unreliable	**5**	Improbable
F	Cannot Be Judged	**6**	Cannot Be Judged

Source: RMS Threat Communication Operating Procedures.

However, because RMS has historically only further disseminated to financial institutions threat information created by known and reliable sources, such as that developed by CISA and the United States Department of the Treasury (Treasury Department), this information is already considered accurate and reliable. Further,

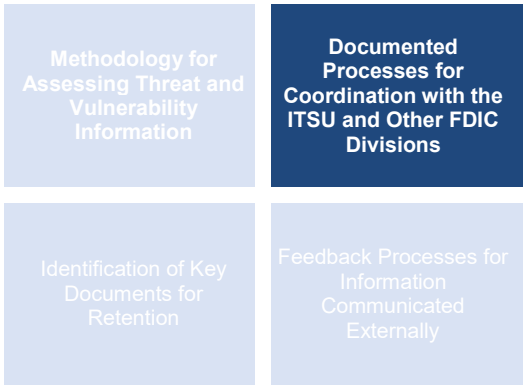
[62] Trusted and reliable sources of threat and vulnerability information include CISA and the FBI. The FDIC has shared other specific threat and vulnerability information with financial institutions during zero-day vulnerabilities as discussed throughout this report.
[63] The FDIC adopted this methodology from another federal financial regulator.

should the FDIC generate threat information internally from its examination activities, this information would presumably be considered accurate and reliable. As a result, the methodology within the RMS Threat Communication Operating Procedures may not be the most appropriate for the FDIC and may create inefficiencies when determining whether to share threat and vulnerability information with financial institutions. For example, RMS officials may spend time unnecessarily completing steps when information is already considered reliable and sufficient.

RMS officials noted that they are updating their Threat Communication Operating Procedures and agreed that the current methodology did not align with the threat and vulnerability information they communicate to financial institutions. RMS officials stated that they integrated the methodology in their Threat Communication Operating Procedures because it was determined to be the best methodology available when the procedures were initially developed.

Documented Processes for Coordination with the ITSU and Other FDIC Divisions

The ISP Charter and ITSU Standard Operating Procedure establish the importance of coordination and defines two-way communication between ITSU analysts and Division and Office subject matter experts. For example, the ISP Charter states that Divisions and Offices must articulate their threat information needs and Division and Office subject matter experts shall participate in quarterly ISP meetings to collaborate and share threat and vulnerability-related information.



According to ITSU and RMS officials, they are collaborating regularly and sharing threat information. For example, according to RMS officials, they have weekly meetings with the ITSU to discuss mutual interests, and RMS shares its weekly Cybersecurity Brief with the ITSU. However, we found that the RMS Threat Communication Operating Procedures do not define the processes to ensure there is effective coordination and communication with the ITSU or other FDIC Divisions and Offices that may obtain or have a need for threat and vulnerability information. Specifically, although the FDIC has established the ITSU with responsibility for threat information acquisition, analysis, and production, RMS has not updated its threat sharing policies, procedures, and/or processes to fully incorporate the ITSU. For example, RMS has not incorporated the ITSU into its processes or procedures to ensure that the ITSU receives relevant threat and vulnerability information obtained

through the FDIC's Computer-Security Incident Notification Rule. In addition, RMS officials confirmed they had not shared any such incident information with the ITSU.

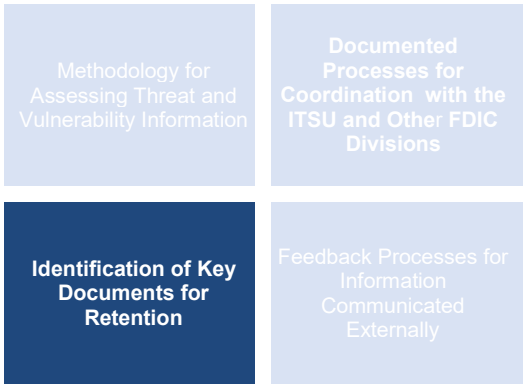
Further, while it may occur infrequently, RMS can obtain threat and vulnerability information related to specific banks from another FDIC Division or Office. For example, RMS obtained vulnerability information specifically related to an FDIC-supervised institution's public web server through the Chief Information Officer Organization (CIOO) under the FDIC's Vulnerability Disclosure Policy (VDP).[64] Over a period of 24 days, this information was communicated to the FDIC Region, and FDIC examination staff appropriately shared this vulnerability information with the financial institution. However, the RMS Threat Communication Operating Procedures do not account for a process for such communications or for obtaining information from other FDIC Divisions or Offices that may require targeted communication to banks.

Without consistently documented processes and procedures for coordinating with the ITSU, RMS may miss opportunities to enhance the threat data it receives with information or intelligence that the ITSU may independently maintain or have access to. For example, financial institutions report critical computer-security incidents and notification incidents to RMS. This information may be further enhanced based on the ITSU's access to classified sources in an effort to determine the extent or significance of the threat to the financial sector. Additionally, without documented procedures for coordinating and receiving threat information from other Divisions, such as through the CIOO's VDP, RMS may not consistently and timely provide relevant and actionable threat and vulnerability information to financial institutions.

RMS officials acknowledged that while regular communication and coordination was occurring with the ITSU, the processes had not been formalized in their Threat Communication Operating Procedures because they were drafted and implemented before ITSU's policies were formalized. Finally, RMS officials acknowledged that in rare occasions they may receive information from other FDIC Divisions that requires external communication to financial institutions. We determined that specific processes for addressing these events were not formalized in their procedures.

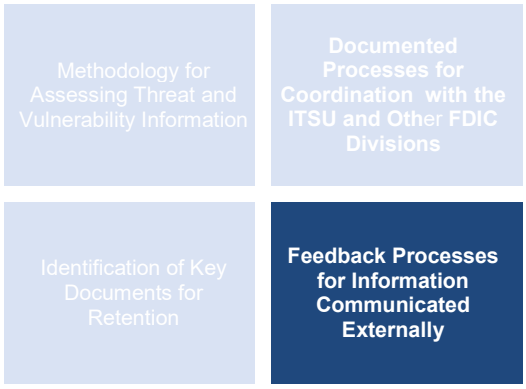
[64] In accordance with OMB M-20-32 *"Improving Vulnerability Identification, Management, and Remediation*" and CISA's Binding Operational Directive (BOD 20-01), the FDIC provides assurance that good faith security research is welcomed and authorized via the FDIC Vulnerability Disclosure Policy (https://www.fdic.gov/policies/vulnerability/). Vulnerability disclosure is the act of initially providing vulnerability information to a party that was not believed to be previously aware.

Identification of Key Documents for Retention



The "Recordkeeping" section of the RMS Threat Communication Operating Procedures provides guidance for where to store "documentation of use of these procedures." However, the RMS Threat Communication Operating Procedures do not list key documents that should be retained in order to support RMS threat sharing decisions. During our evaluation, we selected a small judgmental sample of instances where RMS documented its use of the procedures and found that an RMS official maintained consistent documentation, including responses to the four questions detailed above, as well as copies of the completed source reliability and rating document. As a result, we did not find weaknesses regarding the type of documentation that was maintained. However, to address continuity in the event of changing personnel and to ensure consistency, the procedures should be updated to specify the documentation that must be maintained. RMS officials acknowledged that additional clarification could be provided within their procedures on the key documents for retention to support RMS threat sharing decisions.

Feedback Processes for Information Communicated Externally



We determined that RMS has not established a feedback process for threat and vulnerability information shared externally with financial institutions. According to NIST 800-150, organizations should increase the usefulness and effectiveness of threat information by obtaining feedback. The Department of Homeland Security (DHS) Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community (October 2016) further 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."

In October 2022, RMS issued an RD memorandum[65] focused on threat information sharing internally within the FDIC. Specifically, the October memorandum formalized procedures for measuring the utility and effectiveness of threat information used and shared internally within the FDIC to support the supervision program. Within the RD memorandum, RMS established the tools it will use to collect feedback and measure effectiveness, including: surveys, related evaluations, and product reviews. The FDIC's ITSU has also integrated feedback processes into its threat information sharing operations. (b) (7)(E)

The FDIC ITSU is developing electronic customer feedback forms and staff will engage with FDIC stakeholder recipients of distributed threat information products to determine whether stakeholder requirements and expectations were met.

According to RMS officials, they have not requested feedback from financial institutions because the originators of the threat information that the FDIC is further disseminating already ask for, or receive, feedback. RMS officials added that they did not want to burden financial institutions by requesting feedback multiple times on the same information. RMS officials further stated that they have not requested feedback from banks because of the requirements under the Paperwork Reduction Act. Specifically, RMS officials noted that a request for feedback would require notice and comment under the Paperwork Reduction Act if it involved more than nine institutions. In addition, RMS officials indicated that obtaining feedback would require significant resources that are better allocated to examinations and policy. RMS officials acknowledged that feedback may be needed if the FDIC was regularly developing its own original threat information products.

Without defined mechanisms to obtain feedback, RMS may miss opportunities to improve its external threat information sharing processes and ensure that financial institutions receive actionable and relevant threat and vulnerability information.

[65] RMS RD Memorandum 2022-030 *Measuring the Utility and Effectiveness of Threat Information Used to Support the Supervision Program,* October 24, 2022.

Recommendations

We recommend the Director, RMS:

6. Update the Division of Risk Management Supervision Threat and Vulnerability Communication Operating Procedures to:
   (1) account for a more appropriate methodology for determining when to share threat and vulnerability information created internally and by other credible sources;

   (2) formalize processes for (a) coordinating with the Intelligence and Threat Sharing Unit and accounting for threat and vulnerability information received from the Intelligence and Threat Sharing Unit, (b) coordinating with the Chief Information Officer Organization under the Vulnerability Disclosure Policy program, and (c) coordinating with other FDIC Divisions and Offices that may obtain relevant threat and vulnerability information that requires communication to financial institutions; and

   (3) specify the key documents that should be retained to support the Division of Risk Management Supervision threat sharing decisions.

7. Develop and implement a feedback process for external threat sharing activities.

Performance Measures for External Threat Sharing

The GAO has routinely found that performance measures show the progress agencies make toward achieving program goals.[66] According to the GAO, 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 related measures as key parts of an effective internal control system.

RMS has not developed performance measures or metrics to assess their efforts in sharing threat and vulnerability information externally with financial institutions. Specifically, the RMS Operational Risk group has not established any metrics to measure the effectiveness of its external threat and vulnerability information sharing activities, including (1) the number of threat products distributed or the (2) timeliness

[66] 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).

of threat product dissemination to meet financial institution needs. Such metrics would be comparable to the KPIs for the FDIC's internal threat sharing operations established by the ITSU.

In response to the recommendations from our previous report,[67] (b) (7)(E)

Table 5 presents (b) (7)(E)

Table 5: (b) (7)(E)

• (b) (7)(E)
• (b) (7)(E)

Source: (b) (7)(E)

RMS officials indicated that while they have initiated discussions around developing metrics to measure RMS performance on external threat sharing activities, they have not been formally established. An RMS official noted challenges in determining what they would measure, the indicators of performance, and how to obtain the related information. RMS staff stated that another challenge related to measuring timeliness is that timing depends on the significance of the threat. An RMS official noted that tiered metrics for timeliness based on criticality of the message may be appropriate.

RMS officials also stated that performance metrics are appropriate for the ITSU mission but would not be appropriate for the RMS mission. RMS officials felt that developing performance metrics and the work required to gather the information to measure their performance would require additional work with limited value. RMS officials also stated that they would rather devote time to FDIC examination activities than commit resources to something not seen as mission priority. As such, RMS officials indicated that they considered actions that would be more aligned with the FDIC mission and not overly burdensome. For example, RMS officials stated they could measure (1) bank participation in threat information sharing groups such as the FS-ISAC or (2) the speed with which other organizations provide threat information to banks.

We believe that absent performance metrics, like those developed by the ITSU ISP for internal threat sharing, RMS has limited ability to effectively measure the performance and success of its external threat information sharing activities. Without evidence-based performance information, the FDIC's ability to make informed

[67] FDIC OIG, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (AUD-22-003) (January 2022).

decisions about how to improve its external threat information sharing processes and activities is limited.

Further, the resource limitations expressed by RMS highlight a growing concern within the FDIC's bank examination and supervision activities. Specifically, we note that the recent Report by the FDIC on the failure of Signature Bank[68] disclosed historic examiner resource constraints within its large bank Continuous Examination Process. Further, the OIG's Top Management and Performance Challenges report for the FDIC cites resource management concerns in many FDIC Divisions and Offices.[69] Without adequate resource management, the FDIC may not be able to carry out all of its related mission duties and functions.

Recommendations

We recommend the Director, RMS:

8. Develop performance measures to assess the effectiveness of its external threat and vulnerability information sharing activities.

9. Evaluate and, if necessary, obtain the resources needed for the timely implementation of the recommendations in this report to further mature the FDIC's threat information sharing program.

[68] FDIC, FDIC's Supervision of Signature Bank (April 28, 2023).
[69] FDIC OIG, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (February 2023).

Enhancing FDIC Capabilities to Identify Threat and Vulnerability Information

RMS has previously leveraged a natural language processing tool[70] to conduct analysis of unstructured data from FDIC examination information during previous zero-day attacks. By utilizing this resource, RMS was able to successfully identify banks that warranted FDIC contact based on relevant risk and complexity characteristics. For example, during the FDIC's response to the "Spectre" and "Meltdown"[71] vulnerabilities, RMS used natural language processing techniques to identify financial institutions with patch management weaknesses that may be more susceptible to these attacks. Further, during the FDIC's response to the Solar Winds[72] and Apache Log4j[73] vulnerabilities, RMS was able to identify financial institutions with weaknesses in the areas of threat monitoring, risk assessment, or patch management and where examiners specifically mentioned "Solar Winds" or "Apache" in FDIC examination work papers. By leveraging the capabilities of natural language processing techniques in these instances, RMS was then able to direct its communications to financial institutions that warranted FDIC contact based on relevant risk and complexity characteristics. RMS has not utilized natural language processing techniques for threat and vulnerability information trending and analysis beyond the aforementioned zero-day attacks.

> *A zero-day attack is an attack that exploits a previously unknown hardware, firmware, or software vulnerability.*
>
> **NIST Interagency Report 8011 Vol. 3 Automation Support for Security Control Assessments Software Asset Management (December 2018)**

To support the continued use of natural language processing techniques, according to FDIC officials, in 2023 the FDIC dedicated a budget for an Artificial Intelligence/Machine Learning/Natural Language Processing solution. Prior to 2023, FDIC officials stated that FDIC resources and contractor support for these efforts were inconsistent. Specifically, they indicated that the budget supporting the FDIC's natural language processing tool fluctuated and contractor support resources turned

[70] The FDIC developed the natural language processing tool – AlphaREX - in house with the support of contractors in 2017.
[71] On January 3, 2018, the National Cybersecurity and Communications Integration Center became aware of a set of security vulnerabilities—known as Spectre and Meltdown—that affected modern computer processors. These vulnerabilities could be exploited to steal sensitive data present in a computer system's memory.
[72] In 2020, CISA issued Emergency Directive 21-01 as it was identified that SolarWinds Orion products were being exploited by malicious actors. The vulnerability permitted attackers to gain access to network-traffic management systems.
[73] In 2021, CISA issued Emergency Directive 22-02 as a series of vulnerabilities in the popular Java-based logging library Log4j were under active exploitation by multiple threat actors. The vulnerabilities allowed an unauthenticated attacker to remotely execute a code on a server.

over frequently. According to an RMS official, the turnover in specialized contractor resources caused several impacts to furthering the FDIC's natural language processing efforts, including:

(1) Addressing the changes in expertise of the developers;
(2) Delays from the additional time needed to onboard and integrate contractors; and
(3) Delays from re-work and correcting errors.

According to an RMS official, this impacted the FDIC's ability to progress on established use cases or apply natural language processing techniques to other unstructured data sets available within the FDIC. The FDIC's threat intelligence operations may benefit from using the current natural language processing tool or alternative capabilities to analyze other unstructured data sets for the identification of threat and vulnerability information.

FDIC Unstructured Data Sets

The Division of Depositor and Consumer Protection (DCP) manages the consumer complaint process within the FDIC and maintains the Enterprise Public Inquiries and Complaints (EPIC) system to record the consumer complaints it receives.[74] During our evaluation, DCP officials confirmed that while such instances may be rare, the correspondence from complainants may include whistleblower allegations from bank insiders, threat and vulnerability information such as physical threats to FDIC staff, physical threats to banks, and/or allegations of weak information systems or controls. In addition, our review of the data from the EPIC system identified a number of complaints related to Cyber and Fraud - the top threats to banks identified by our survey of financial institutions. The trending and analysis of such data using natural language processing may help inform FDIC threat intelligence officials on relevant fraud-related information and cybersecurity risks. Ultimately, this information if communicated externally, could inform key officials at banks, such as Bank Secrecy Act / Anti-Money Laundering (BSA/AML) Officers, Chief Information Officers, and Chief Information Security Officers of relevant threats.

In addition, as previously discussed in this report, the FDIC can obtain threat and vulnerability information through the CIOO under the FDIC's VDP. While this may occur infrequently, this could serve as another data set for which the FDIC could use natural language processing to better inform their threat intelligence efforts.

Other FDIC Divisions may also benefit from the FDIC's natural language processing capabilities. For example, as highlighted in the September 2022 issue of the FDIC Artificial Intelligence/Machine Learning Newsletter, the Division of Resolutions and

[74] EPIC is an FDIC enterprise database used for tracking, reporting, and responding to consumer correspondence.

Receiverships (DRR) and its newly formed Modeling & Analytics team disclosed its interest in exploring natural language processing capabilities to unlock valuable insights to support DRR's operational readiness. Further, the DOA ITSU is responsible for identifying relevant threat information databases and sources and sharing intelligence products aligned to the FDIC's threat information needs. The FDIC's Senior Intelligence Officer (SIO) within the ITSU is specifically responsible for identifying emerging trends and producing timely intelligence products for dissemination to FDIC senior leaders and staff as well as field stakeholders. As a result, the DOA ITSU may benefit from using natural language processing capabilities to identify and analyze information available throughout the FDIC in support of its responsibilities. During this evaluation, the DOA ITSU developed a list of internal and external threat information data sources and, based on our work, added both EPIC and the FDIC's VDP as sources to the list. However, other FDIC data sets may contain relevant threat and vulnerability information. An ITSU official confirmed that ITSU would consider all relevant threat information in FDIC holdings.

Expanded use of natural language processing techniques and capabilities within the FDIC and these aforementioned unstructured data sets could inform and improve its threat intelligence operations and ultimately provide valuable information for financial institutions.

Recommendation

We recommend the FDIC Director of RMS in coordination with FDIC Chief, ITSU:

10. Ensure that all data sets within the FDIC that contain relevant threat and vulnerability information are assessed and natural language processing or alternative technological capabilities are considered for enhancing threat and vulnerability information sharing operations.

FDIC COMMENTS AND OIG EVALUATION

The FDIC's Director, Division of Risk Management Supervision (RMS), provided a written response, dated August 10, 2023, to a draft of this report. In its response, the FDIC reiterated the importance for banks and their service providers to effectively use threat and vulnerability information to defend their operations. The FDIC also stated that it is rarely an originator of threat and vulnerability information and that it promotes the importance that banks and service providers receive this information from the originator or from other entities that compile such information. The response is presented in its entirety in Appendix 4.

The FDIC concurred with the report's recommendations. The FDIC plans to complete corrective actions for these recommendations by March 31, 2024. We

consider all 10 recommendations to be resolved. All of the recommendations in this report will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions is contained in Appendix 5.

Objective

The evaluation objective was to determine whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information.

We conducted this evaluation from August 2022 through July 2023 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). These standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objective. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objective.

Scope and Methodology

The scope of the evaluation focused on the FDIC's efforts to implement effective processes to ensure that financial institutions receive clear, actionable, and timely threat and vulnerability information. Specifically, we assessed the FDIC's computer-security incident notification procedures and practices, incidents reported by banks and entered into ViSION, and the FDIC's InTREx program and areas for assessment of bank threat intelligence programs. In addition, we evaluated the procedures and processes in place for acquiring, analyzing, and disseminating threat and vulnerability information to financial institutions. Further, we assessed any efforts and tools in place to analyze and trend unique FDIC data and information from examinations or other sources.

To obtain an understanding of the FDIC's processes for external threat and vulnerability information sharing with financial institutions and to address the evaluation objective, we interviewed FDIC personnel from the Division of Risk Management Supervision (RMS), including the Deputy Director and other officials within RMS's Operational Risk group, and the Associate Directors from the IT Supervision and AML & Cyber Fraud Branches. We also interviewed officials from the DOA, including the Deputy Director of DOA's Corporate Services Branch, the Personnel Security Unit Chief within the Security Enterprise Programs Section (SEPS), the Principal Assistant Director of DOA's SEPS, and the ITSU Chief.

Further, we received feedback from other FDIC Divisions and Offices regarding threat and vulnerability information received based on the different Division and Office missions and responsibilities. This included the Division of Complex Institution

Supervision and Resolution (CISR), the DCP, the CIOO, the DRR, and the Division of Insurance and Research (DIR). We assessed whether this information was relevant and helpful for financial institutions and determined whether it was shared, as appropriate.

We reviewed relevant FDIC policies, procedures, and guidance, including:

- FDIC RMS Regional Directors (RD) Memoranda:
  - Information Technology Risk Examination (InTREx) Program, 2016-009-RMS (June 2016);
  - RMS Threat and Vulnerability Communication Operating Procedures, 2022-017-RMS (July 2022);
  - Computer-Security Incident Response Procedures, 2022-021-RMS (August 2022);
  - Measuring the Utility and Effectiveness of Threat Information Used to Support the Supervision Program, 2022-030-RMS (October 2022);
- FDIC RMS Regional Computer-Security Incident Response Guide (June 2022);
- FDIC RMS Computer Security Incident Response Plan (June 2022);
- ViSION Security Incident Enhancements and Help Documents;
- FDIC Directive 1600.09 Intelligence and Counterintelligence Programs (December 2022);
- FDIC DOA Standard Operating Procedures:
  - Threat Information Acquisition, Analysis, Production, Dissemination, and Storage (December 2022);
  - Developing, Approving and Maintaining Standing Information Needs and Key Intelligence Questions (December 2022);
- FDIC Intelligence Support Program Charter;
- FDIC Calendar Year (CY) 2023 Standing Information Needs and Key Intelligence Questions (December 2022); and
- FDIC Vulnerability Disclosure Policy (VDP) (June 2022).

In addition, we reviewed applicable laws, policies, procedures, and guidance related to FDIC examinations of financial institutions as well as those of other Federal regulators. We also selected a small sample of external threat sharing activities to determine whether RMS followed its Threat and Vulnerability Communication Operating Procedures. We reviewed the FDIC's Risk Profile and Risk Inventory from April 2022 to May 2023 to determine if there were any Agency risks related to the objective. Finally, we reviewed the RMS (b) (7)(E), (b) (8) (December 2022).

To assess the FDIC's external threat and vulnerability sharing efforts with financial institutions, we used the FDIC RMS RD Memoranda, the FDIC's ISP Charter and

Directives, and the FDIC's computer-security incident response guidance. We supplemented the FDIC's internal documents with the following additional criteria:

- *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (National Plan);
- Financial Services Sector-Specific Plan (2015);
- *Sound Practices to Strengthen Operational Resilience* (Sound Practices Paper) (October 2020);
- GAO's *Standards for Internal Control in the Federal Government* (September 2014);
- DHS *Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community* (October 2016);
- NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing* (October 2016); and
- OIG and GAO reports and recommendations.

We interviewed officials from the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the National Credit Union Administration (NCUA) to understand whether, and how, they use internal information, including that from examinations, to identify threat and vulnerability-related trends and patterns that could be shared with financial institutions. We also obtained an understanding of related policies and procedures addressing whether, and how, OCC, FRB, and NCUA share information with financial institutions. In addition, to develop best practices, we interviewed officials from the Department of Transportation's Federal Aviation Administration Threat Analysis Division to understand their threat sharing operations with external non-government stakeholders they are responsible for regulating.

We also interviewed and coordinated with four banking associations to conduct an anonymous survey of a representative set of financial institutions. The survey obtained feedback from banks on whether the threat information received from the FDIC and other Federal regulators is sufficient, adequate, timely, relevant, and actionable. The survey also solicited comments from banks to determine whether the FDIC can improve its external threat sharing operations. We received responses from 33 financial institutions in whole or in part to the survey questions.

Appendix 2

Acronyms and Abbreviations

AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
CISR	Division of Complex Institution Supervision and Resolution
CFT	Countering the Financing of Terrorism
CY	Calendar Year
DCP	Division of Depositor and Consumer Protection
DHS	Department of Homeland Security
DIR	Division of Insurance and Research
DOA	Division of Administration
DRR	Division of Resolutions and Receiverships
EPIC	Enterprise Public Inquiries and Complaints
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIL	Financial Institution Letter
FinCEN	Financial Crimes Enforcement Network
FRB	Federal Reserve Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSOC	Financial Stability Oversight Council
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
GAO	Government Accountability Office
InTREx	Information Technology Risk Examination
ISP	Intelligence Support Program
IT	Information Technology
ITSU	Intelligence and Threat Sharing Unit
KPI	Key Performance Indicator
NCUA	National Credit Union Administration
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
RCIRG	Regional Computer-Security Incident Response Guide
RD	Regional Directors
RMS	Division of Risk Management and Supervision
ROE	Report of Examination

SAR	Suspicious Activity Report
SEPS	Security Enterprise Programs Section
SIO	Senior Intelligence Officer
SSP	Significant Service Providers
VDP	Vulnerability Disclosure Policy
ViSION	Virtual Supervisory Information on the Net

Level	General Definition	Regional Office Escalation	Timing*
Level 5 *Emergency* **(Black)**	An incident or series of incidents *poses an active or imminent* threat of sector-wide outage(s) and/or *catastrophically destructive compromises* to IDIs and SPs, with nearly certain likelihood of catastrophic damage resulting in a potential collapse of the capital markets, payment, clearing, or settlement services, or nationwide loss of public confidence in the financial system.	WO Regional federal and state regulators Other FDIC regional divisions and offices	Immediate Notification
Level 4 *Severe* **(Red)**	An incident or series of incidents *likely to result in a sector-wide outage(s) or significant destructive compromises* to IDIs and SPs, with at least roughly even odds to lead to significant adverse impact to capital markets, payment, clearing, or settlement services for a majority of IDIs with associated impact to consumer confidence.	WO Regional federal and state regulators Other FDIC regional divisions and offices	Immediate Notification
Level 3 *High* (Orange)	*Likely to result in demonstrable and observable* negative or adverse impact to critical operations of IDIs and SPs, or at least roughly even odds of isolated run(s) on the IDIs by personal or corporate IDI customers, or the possibility of a regional/national disruption to capital markets, payment, clearing, or settlement services. Consumer confidence directly impacted by an incident that compromises day-to-day banking or financial operations.	WO Regional federal and state regulators Other FDIC regional divisions and offices	Notification within 2 hours
Level 2 *Medium* (Yellow)	*May impact and disrupt* financial services operations of one or more IDIs or SPs. Likely damage or disruption to critical operations at a single IDI or SP, or non-critical operations at several IDIs, or compromise of several firms' confidential data with potential to be mitigated quickly.	WO Regional federal and state regulators as deemed necessary Other FDIC regional divisions and offices as deemed necessary	Notification within 24 hours
Level 1 *Low* (Green)	*Unlikely to impact* financial services operations of IDIs or SPs and indicates localized, contained compromise or disruption of an IDI. No exploits have been identified, or exploits have been identified but no significant damage, disruption or system compromise has occurred.	FO, RO, or WO level where it was initially reported with wide latitude whether or not to escalate further.	Discretionary
Level 0 Baseline (White)	Unsubstantiated or inconsequential event. There are many incidents in this category and the examiner should be aware of them for purposes of evaluating information security program adequacy.	Not warranted	Not warranted

Federal Deposit Insurance Corporation

MEMO

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

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

CC: Daniel H. Bendler, Deputy to the Chairman and Chief Operating Officer, Division of Administration
E. Marshall Gentry, Chief Risk Officer
Martin D. Henning, Deputy Director, Division of Risk Management Supervision
Lisa D. Arquette, Associate Director, Division of Risk Management Supervision

DATE: August 10, 2023

RE: Management Response to the OIG Draft Audit Report, Sharing of Threat and Vulnerability Information with Financial Institutions (No. 2022-008)

The FDIC 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 July 27, 2023. FDIC management concurs with the report's ten recommendations. FDIC responses to the audit findings and each recommendation are described below.

It is important that banks and their service providers use threat and vulnerability information effectively to defend their operations, that there are high quality threat and vulnerability information sources, and that the FDIC amplify threat and vulnerability information when warranted. The FDIC promotes the importance of threat monitoring programs through multiple venues.[1] The FDIC also monitors multiple high quality threat and vulnerability information sources, both government and private sector sources.[2] The FDIC amplifies threat information when warranted such as when the FDIC and the other Federal Financial Institutions Examination Council (FFIEC) members hosted a webinar for financial institutions

[1] Examples include: the Updated *FFIEC Cybersecurity Resource Guide for Financial Institutions*, September 2022, https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf; and the *FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center*, November 3, 2014, https://www.ffiec.gov/press/pr110314.htm.

[2] Government sources include the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Financial Crimes Enforcement Network. Private sector sources include the Financial Services-Information and Sharing Analysis Center, https://www.fsisac.com/, and the Global Resilience Federation, https://www.grf.org/.

Federal Deposit Insurance Corporation

regarding ransomware attacks affecting banks.[3] Finally, FDIC examiners review the quality of financial institution threat monitoring and provide feedback in the report of examination when threat monitoring is inadequate.

The FDIC is rarely an originator of threat and vulnerability information useful to many banks because of the nature of the information used in supervision, and because examinations are infrequent relative to the quickly changing threat and vulnerability environment. Threat and vulnerability information is originated by other government agencies such as the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the United States Secret Service, the Financial Crimes Enforcement Network, the National Oceanic and Atmospheric Administration, and state and local governments. Therefore, the FDIC promotes the importance of banks and service providers receiving threat and vulnerability information directly from the originator, or from entities that compile information such as the Financial Services Information Sharing and Analysis Center. An example of this promotion is the outstanding FFIEC *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*.[4]

The FDIC's supervision function produces risk management feedback to banks and service providers regarding the above principles when appropriate, but does not generally produce unique threat information. These facts notwithstanding, the FDIC will take action consistent with the OIG's recommendations to increase the probability that any unique threat information the FDIC discovers is shared appropriately.

Management Response to the OIG Recommendations

Recommendation 1: We recommend the FDIC Director of RMS:

Share threat and vulnerability information that is uniquely developed or summarized by the FDIC with financial institutions or other financial sector entities to further strengthen their threat intelligence activities. This includes results from the FDIC's 2022 Ransomware Horizontal Review and relevant trending and analysis conducted by the Division of Risk Management Supervision.

Management Decision: Concur

Planned Action:

The FDIC has shared the results of the ransomware horizontal review multiple times in public presentations, and conveyed to the OIG its plan to share the referenced ransomware review results in a public written report. The FDIC will complete that project. The FDIC will also initiate regular publication of incident data as appropriate, such as certain of the data

[3] FFIEC *Ransomware Financial Sector Trends* Webinar, November 18, 2021. At this webinar, the Financial Crimes Enforcement Network discussed ransomware trends and it's Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, November 8, 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[4] The Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement, https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf

FDIC Federal Deposit Insurance Corporation

presented in internal reports.

Estimated Completion Date: December 31, 2023

Recommendation 2: We recommend the FDIC Director of RMS:

Conduct training for examiners on the requirements for recording computer-security incidents, the information to include, and specific requirements for Notification Rule incidents.

Management Decision: Concur

Planned Action:

The FDIC will add requirements for recording computer-security incidents to the *Introduction to Security* course materials. All examiners are required to take this course.

Estimated Completion Date: March 31, 2024

Recommendation 3: We recommend the FDIC Director of RMS:

Improve controls over the intake and recording of computer-security incidents reported by banks and service providers to ensure that: (1) records are added to ViSION as required, (2) recorded incident information in ViSION and in RMS Incident Reports is complete, appropriate, and accurate, and (3) the most severe incidents can be readily identified to promote early awareness of emerging threats.

Management Decision: Concur

Planned Action:

The FDIC will add incident data quality checks to the scope of all regional reviews, and will publicize to all regions any material deficiencies identified in a regional review. This will lower the risk that incidents are erroneously categorized as critical in ViSION when they are not.

Estimated Completion Date: December 31, 2023

Recommendation 4: We recommend the FDIC Director of RMS:

Conduct a review of computer-security incidents reported since May 1, 2022, to ensure ViSION records are complete and accurate.

Management Decision: Concur

Federal Deposit Insurance Corporation

Planned Action:

The FDIC will conduct the recommended review.

Estimated Completion Date: December 31, 2023

Recommendation 5: We recommend the Director, RMS in coordination with ITSU:

Ensure FDIC threat and vulnerability communication procedures facilitate the sharing of unclassified non-cyber related threat and vulnerability information.

Management Decision: Concur

Planned Action:

The FDIC will update procedures to facilitate the sharing of unclassified non-cyber related threat and vulnerability information identified by the FDIC.

Estimated Completion Date: March 31, 2024

Recommendation 6: We recommend the FDIC Director of RMS:

Update the RMS Threat and Vulnerability Communication Operating Procedures to:

1. account for a more appropriate methodology for determining when to share threat and vulnerability information created internally and by other credible sources;
2. formalize processes for:
    a. coordinating with the ITSU and accounting for threat and vulnerability information received from the ITSU,
    b. coordinating with the CIOO under the VDP (Vulnerability Disclosure Policy) program, and
    c. coordinating with other FDIC Divisions and Offices that may obtain relevant threat and vulnerability information that requires communication to financial institutions; and
3. specify the key documents that should be retained to support RMS threat sharing decisions.

Management Decision: Concur

Planned Action:

The FDIC will update and simplify the RMS Threat and Vulnerability Communication Operating Procedures to remove the unnecessary complexity in appendices. The updates

Federal Deposit Insurance Corporation

will also specify coordination between RMS, ITSU, the CIOO, and other divisions and offices. Finally, the update will specify what is to be saved relative to the discretion exercised.

Estimated Completion Date: March 31, 2024

Recommendation 7: We recommend the FDIC Director of RMS:

Develop and implement a feedback process for external threat sharing activities.

Management Decision: Concur

Planned Action:

The FDIC will solicit feedback regarding threat amplification messages to banks and service providers typically sent through FDIC*connect*, and any other threat message to banks.

Estimated Completion Date: March 31, 2024

Recommendation 8: We recommend the FDIC Director of RMS:

Develop performance measures to assess the effectiveness of its external threat and vulnerability information sharing activities.

Management Decision: Concur

Planned Action:

As specified in the response to Recommendation 7, the FDIC will solicit feedback and develop measures to assess information sharing effectiveness.

Estimated Completion Date: March 31, 2024

Recommendation 9: We recommend the FDIC Director of RMS:

Evaluate and, if necessary, obtain the resources needed for the timely implementation of the recommendations in this report to further mature the FDIC's threat information sharing program.

Management Decision: Concur

Planned Action:

The actions specified in this report will be completed with the resources approved by the

FDIC Federal Deposit Insurance Corporation

FDIC's Board of Directors. The FDIC's annual budgeting process includes division and office director consideration of any OIG or GAO audit recommendations that may require additional resources or funding to implement.

Estimated Completion Date: March 31, 2024

Recommendation 10: We recommend the Director, RMS in coordination with ITSU:

Ensure that all data sets within the FDIC that contain relevant threat and vulnerability information are assessed and natural language processing or alternative technological capabilities are considered for enhancing threat and vulnerability information sharing operations.

Management Decision: Concur

Planned Action:

The FDIC will continue using appropriate technologies to assess the data it has to identify threat and vulnerability information to share. ITSU documents that identify possible research datasets will be evaluated annually, and updated as necessary. As part of this effort, ITSU will periodically prepare and update an inventory of documents and sources that contain datasets used to identify threat and vulnerability information considered to be worth sharing.

Estimated Completion Date: March 31, 2024

Appendix 5 Summary of the FDIC's Corrective Actions

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	RMS will share the referenced ransomware horizontal review results in a public written report. The FDIC will also initiate regular publication of incident data as appropriate, such as certain data presented in internal reports.	December 31, 2023	$0	Yes	Open
2	The FDIC will add requirements for recording computer-security incidents to the Introduction to Security course materials, required to be completed by all examiners.	March 31, 2024	$0	Yes	Open
3	The FDIC will add incident data quality checks to the scope of all regional reviews, and will publicize to all regions any material deficiencies identified in a regional review.	December 31, 2023	$0	Yes	Open
4	The FDIC will conduct a review of computer-security incidents reported since May 1, 2022, to ensure ViSION records are complete and accurate.	December 31, 2023	$0	Yes	Open
5	The FDIC will update procedures to facilitate the sharing of unclassified non-cyber related threat and vulnerability information identified by the FDIC.	March 31, 2024	$0	Yes	Open
6	The FDIC will update and simplify the RMS Threat and Vulnerability Communication Operating Procedures to: (1) remove the unnecessary complexity in appendices, (2) specify coordination between RMS, ITSU, the CIOO, and other divisions and offices, and (3) specify what information is to be saved relative to the discretion exercised.	March 31, 2024	$0	Yes	Open
7	The FDIC will solicit feedback regarding threat amplification messages to banks and service providers typically sent through FDICconnect, and any other threat message to banks.	March 31, 2024	$0	Yes	Open
8	The FDIC will solicit feedback and develop measures to assess information sharing effectiveness.	March 31, 2024	$0	Yes	Open

9	The FDIC will complete the actions specified in this report with the resources approved by the FDIC's Board of Directors.	March 31, 2024	$0	Yes	Open
10	The FDIC will continue using appropriate technologies to assess its data for threat and vulnerability information. The FDIC will also evaluate ITSU documents that identify possible research datasets annually and update the documents as necessary. As part of this effort, ITSU will periodically prepare and update an inventory of documents and sources that contain datasets used to identify relevant threat and vulnerability information.	March 31, 2024	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the OIG agrees the planned corrective action is consistent with the recommendation.
2. Management does not concur or partially concurs with the recommendation, but the OIG agrees that the proposed corrective action meets the intent of the recommendation.
3. For recommendations that include monetary benefits, management agrees to the full amount of OIG monetary benefits, or provides an alternative amount and the OIG agrees with that 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.