Evaluation Report
2023-SR-B-010
June 26, 2023

Board of Governors of the Federal Reserve System

Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2023-SR-B-010, June 26, 2023

Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions

Findings

As part of our scoping efforts, we identified findings and recommendations that we believe the Board of Governors of the Federal Reserve System should implement to enhance the cybersecurity incident response process. We found that the Board can update guidance to clarify the mission and the governance structure of the cybersecurity incident response process. A clearly defined mission and governance structure for the cybersecurity incident response process should help guide the efforts of the parties involved and help enhance the effectiveness of the Board and Federal Reserve Banks' response to cybersecurity incidents.

We also found that the Board and Reserve Banks' responses to cybersecurity incidents have not consistently followed the process prescribed in guidance. In addition, multiple interviewees indicated that some stakeholders in the cybersecurity incident response process are unclear on their roles and responsibilities and that training would be beneficial. Clearly documenting the cybersecurity incident response process and the roles and responsibilities of key stakeholders, and providing training on these topics, will enhance the effectiveness of the Board and Reserve Banks' response when a cybersecurity incident occurs at a supervised institution.

We believe that these enhancements will improve the effectiveness of the cybersecurity incident response process and that the Board should prioritize addressing these items. We are communicating these items at the end of our scoping effort as these items may aid the Division of Supervision and Regulation's (S&R) assessment of refinements to the cybersecurity incident response process as part of its projects to enhance the process.

Recommendations

Our report contains recommendations designed to enhance the cybersecurity incident response process. In its response to our draft report, the Board concurs with our recommendations and outlines actions to address them. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We initiated an evaluation in August 2022 to assess the Board and Reserve Banks' cybersecurity incident response process for supervised institutions. We are issuing this report to communicate our findings and recommendations based on the results of our scoping.

Background

Cybersecurity risks present significant and dynamic challenges to financial institutions. A significant cybersecurity incident at a Board-supervised financial institution could disrupt its operations and ultimately affect financial stability. *Cybersecurity incidents* occur through the use of computer networks and result in an actual or potentially adverse effect on the confidentiality, integrity, or availability of an institution's information systems or the information residing therein.

In response to the increasing frequency and sophistication of cybersecurity incidents at Board-supervised institutions and their service providers, S&R developed a playbook that seeks to establish procedures and protocols for effective, consistent, and replicable supervisory actions in response to cybersecurity incidents.

Recommendations, 2023-SR-B-010, June 26, 2023

Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions

Finding 1: The Board Can Update Guidance to Clarify the Mission and Governance Structure of the Cybersecurity Incident Response Process

Number	Recommendation	Responsible office
1	Update the playbook to clarify the mission and reflect the governance structure of the cybersecurity incident response process. As part of this effort, consider whether the current mission statement aligns with the Board's vision for this process.	Division of Supervision and Regulation
2	Update the oversight plan for CAST to clearly describe the governance structure of the cybersecurity incident response process, including a. the roles and responsibilities of SORP and OR in overseeing the cybersecurity incident response process. b. how decisionmaking authority will be exercised.	Division of Supervision and Regulation
3	Update CAST's operating procedures to reflect the governance structure.	Division of Supervision and Regulation

Finding 2: The Board Can Enhance Guidance and Training on the Cybersecurity Incident Response Process

Number	Recommendation	Responsible office
4	Update the playbook to a. reflect the requirements for financial institutions to report cybersecurity incidents under the Notification Rule and any associated changes to the cybersecurity incident response process or the roles and responsibilities of stakeholders. b. clarify whether references to the severity rating are referring to the institution severity rating or sector severity rating, the process and criteria for changing a severity rating, and how changes to the severity rating affect the cybersecurity incident response procedures staff should follow. c. clarify the requirement for completing an AAR after a cybersecurity incident and the party responsible for completing it. d. clarify the circumstances that warrant informing Board members of a cybersecurity incident.	Division of Supervision and Regulation
5	Update the Board's December 2018 playbook implementing guidance to reflect a. the updates made to the playbook as part of recommendation 4. b. the role of OR in the cybersecurity incident response process. c. the governance structure of the cybersecurity incident response process.	Division of Supervision and Regulation
6	Require that key stakeholders in the cybersecurity incident response process complete training or other exercises on their roles and responsibilities in the process once the updates to the playbook and its implementing guidance have been completed.	Division of Supervision and Regulation

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: June 26, 2023

TO: Michael S. Gibson
Director, Division of Supervision and Regulation
Board of Governors of the Federal Reserve System

FROM: Michael VanHuysen
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Report 2023-SR-B-010: *Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions*

We have completed our report on the subject evaluation. We initiated this evaluation to assess the Board of Governors of the Federal Reserve System and Federal Reserve Banks' cybersecurity incident response process for supervised institutions.

We provided you with a draft of our report for review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address our recommendations. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from the Board and Reserve Banks during our evaluation. Please contact me if you would like to discuss this report or any related issues.

cc: Patrick J. McClanahan
Jennifer Burns
Arthur Lindo
Marta Chaffee
Lisa Ryu
Todd Vermilyea
Richard Naylor
Ray Diggs
Stephen Curren
Matthew Hayduk
Christie Vazquez
Tamara Watkins
Jason Tarnowski
Chad Siegrist

Ann Sommantico
Ricardo A. Aguilera
Cheryl Patterson
Ryan Lordos
Jennifer Herring
Jherylris Herron
Chris Haley
Dianne Dobbeck
William Spaniel
Stephen Jenkins
Lisa White
Joseph Davidson
Julie Williams
Carl White
Christine Gaffney
Tara Humston
Emily Greenwald
Azher Abbasi

Contents

Introduction **7**

Objective 7

Background 7

The Board and Reserve Banks' Role in Supervision 7

Cybersecurity and Financial Institutions 7

Reporting Requirements for Financial Institutions 8

The Cybersecurity Incident Response Process 8

S&R Projects Related to the Cybersecurity Incident Response Process 10

Finding 1: The Board Can Update Guidance to Clarify the Mission and Governance Structure of the Cybersecurity Incident Response Process **12**

Some Staff Do Not Clearly Understand the Roles and Responsibilities of SORP or OR in the Cybersecurity Incident Response Process 12

The Board Can Clarify the Mission of the Cybersecurity Incident Response Process and Its Governance Structure 13

Recommendations 14

Management Response 14

OIG Comment 15

Finding 2: The Board Can Enhance Guidance and Training on the Cybersecurity Incident Response Process **16**

Board and Reserve Bank Cybersecurity Incident Responses Have Not Been Consistent With Guidance 16

Some Stakeholders Indicated That Additional Training Would Be Beneficial 17

The Board Can Update and Enhance Guidance on the Cybersecurity Incident Response Process 17

Recommendations 19

Management Response 19

OIG Comment 20

Appendix A: Methodology **21**

Appendix B: Management Response **22**

Abbreviations **25**

Introduction

Objective

Our objective for this evaluation was to assess the Board of Governors of the Federal Reserve System and Federal Reserve Banks' cybersecurity incident response process for supervised institutions. During our scoping phase, we identified findings and recommendations to enhance the cybersecurity incident response process. We believe that these enhancements will improve the effectiveness of the process and that the Board should prioritize addressing these items. Therefore, we are issuing a report detailing our findings and recommendations following our scoping phase. In addition, we are communicating these items as they may aid the Board's assessment of refinements to the cybersecurity incident response process as part of its projects to enhance the process. Appendix A describes our methodology in greater detail.

Background

The Board and Reserve Banks' Role in Supervision

The Board plays a significant role in supervising and regulating financial institutions. Through its oversight, the Board seeks to ensure that the institutions under its supervisory authority operate in a safe and sound manner and comply with all applicable federal laws and regulations. The Board delegates to each Reserve Bank the authority to supervise certain financial institutions located within the Reserve Bank's district.

The Board's Division of Supervision and Regulation (S&R) leads the Federal Reserve System's supervisory activities. In this role, S&R is responsible for (1) developing regulations and guidance for financial institutions subject to the Board's supervisory authority as well as internal guidance for supervisory staff through its Policy Group and (2) creating, overseeing, and executing supervision programs that promote the safety and soundness of Board-supervised institutions and the financial stability of the U.S. economy through its Supervision Group.

Cybersecurity and Financial Institutions

Cybersecurity risks present significant and dynamic challenges to financial institutions. A significant cybersecurity incident at a Board-supervised financial institution could disrupt its operations and ultimately affect financial stability.[1] In addition, financial institutions increasingly rely on service providers to support their operational and technological infrastructures. A cybersecurity incident at a service provider may present a significant risk to the financial sector because some service providers provide key functions, services, or products to many financial institutions.

[1] *Cybersecurity incidents* occur through the use of computer networks and result in an actual or potentially adverse effect on the confidentiality, integrity, or availability of an institution's information systems or the information residing therein.

Reporting Requirements for Financial Institutions

There are several requirements for financial institutions to report certain cyber and other types of security incidents to their primary federal regulator:

- Supervision and Regulation Letter 05-23, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, directs financial institutions supervised by the Board to promptly contact their Reserve Bank's central point of contact (CPC) to report security incidents involving sensitive customer information.[2] The guidance also requires financial institutions to report security incidents involving sensitive customer information to their primary federal regulator.
- The Computer-Security Incident Notification Rule requires that banking organizations notify their primary federal regulator of any computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's core business lines, critical operations, or ability to deliver banking products and services to a material portion of its customer base, as soon as possible and no later than 36 hours after the banking organization determines that the incident has occurred.[3] This rule went into effect on May 1, 2022.

The Cybersecurity Incident Response Process

In response to the increasing frequency and sophistication of cybersecurity incidents at supervised institutions and their service providers, S&R developed a playbook in April 2018 that seeks to establish procedures and protocols for effective, consistent, and replicable supervisory actions in response to cybersecurity incidents.[4] In addition, in December 2018, the Board issued internal guidance to implement the playbook.

---

[2] The guidance interprets the requirements of section 501(b) of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, and the *Interagency Guidelines Establishing Information Security Standards* to include developing and implementing a response program to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. Sensitive customer information includes a customer's name, address, or telephone number in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or any combination of components of customer information that would allow someone to log in to or access the customer's account.

[3] 12 C.F.R. §§ 225.301(b)(7), 302. The Notification Rule also requires a bank service provider to notify affected banking organization customers as soon as possible when the bank service provider determines that it has experienced an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits, that has materially affected or is reasonably likely to materially affect banking organization customers for 4 or more hours.

[4] For the purposes of the playbook, *supervised institutions* include state member banks; branches and agencies of foreign banks (other than federal branches, federal agencies, and insured state branches of foreign banks); commercial lending companies owned or controlled by foreign banks; Edge Act and agreement corporations; and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). The playbook also applies to savings and loan holding companies that voluntarily report cybersecurity and other types of security incidents. In addition, the playbook applies to the service providers of the above-listed institutions.

The playbook describes the cybersecurity incident response process and establishes expectations for interactions among three primary respondent groups within the System.[5] These groups are the CPC, the Systems and Operational Resiliency Policy (SORP) section, and the Cybersecurity Analytics Support Team (CAST).

- The CPC is the person assigned to lead the supervisory team.[6]
- SORP, located in S&R's Policy Group, is responsible for establishing the policy framework for business technology risk management, including cybersecurity risk management, for supervised institutions.
- CAST, located in the Federal Reserve Bank of Cleveland, is responsible for operating S&R's incident management function; providing situational awareness and reporting on cybersecurity events, incidents, and trends; collecting threat intelligence; and conducting threat monitoring.

In addition to these three groups, the Operational Resilience (OR) function, located in S&R's Supervision Group, plays a key role in the cybersecurity incident response process when a cybersecurity incident occurs at a service provider. OR, established in 2020, is responsible for developing and coordinating an integrated supervisory program for information technology, service providers, and related areas across all supervisory portfolios.[7]

In addition to the roles and responsibilities outlined above, SORP and OR share oversight of CAST. As part of this responsibility, OR developed an oversight plan outlining key expectations for CAST in 2022. Previously, SORP was solely responsible for overseeing CAST.

The cybersecurity incident response process consists of four phases:

1. Incident reporting: Upon receiving an incident report from a financial institution, CAST or the CPC enters the information into the Cyber Event Repository (CER).[8] The creation of a record in the CER notifies CAST, SORP, and other relevant supervisory staff of the cybersecurity incident. OR is notified of all cybersecurity incidents related to service providers.

[5] In addition, the playbook outlines roles for other sections within S&R, other Board divisions, nonsupervisory Reserve Bank functions, and some external agencies and organizations that will participate in the cybersecurity incident response process as necessary.

[6] The CPC role is filled by Reserve Bank officers and examiners who may designate other members of the supervisory team or other supervisory staff to fulfill their responsibilities.

[7] S&R groups its oversight activities into several supervisory portfolios generally based on the total asset size of the institution.

[8] The CER is a data repository and reporting application used to record and track information on cyber and other types of security events reported by supervised institutions. Previously, CPCs were primarily responsible for incident reporting; however, in July 2022, the Board issued internal guidance dividing this responsibility between CAST and CPCs, depending on the incident type.

2. Incident analysis: CAST analyzes the cybersecurity incident, assigns a severity rating, and provides situational awareness reports to relevant stakeholders.[9] Based on the severity level, CAST and SORP may escalate the cybersecurity incident to senior management and other stakeholders. CPCs may also escalate the cybersecurity incident to relevant Reserve Bank groups and the Board's Division of Consumer and Community Affairs.[10]

3. Incident and threat communication and coordination: SORP, with support from CAST and in consultation with key stakeholders, develops and distributes communications for internal and external stakeholders.[11] Such communications can include frequent in-person, teleconference, or email conversations for a single cybersecurity incident. In addition, OR supports CPCs in their supervisory response to cybersecurity incidents at supervised service providers.

4. After action reviews (AAR): For cybersecurity incidents with a severity rating of *medium* or higher, SORP, in consultation with other process participants, develops a report documenting the cybersecurity incident and the response process, including what worked well and what could be improved.

S&R Projects Related to the Cybersecurity Incident Response Process

S&R has initiated internal reviews related to the cybersecurity incident response process. The division enlisted a third-party to perform an independent review of CAST. In October 2021, the third-party issued its report, which identified findings related to governance, communication, training, and the incident management process; it stated that addressing the associated recommendations would enhance CAST's support to the System's supervisory function and other stakeholders.

In January 2022, S&R initiated a project, led jointly by OR and SORP, to enhance the cybersecurity incident response process. According to the project charter, the scope of this effort includes (1) articulating the cybersecurity incident response life cycle; (2) incorporating cybersecurity incident response best practices, lessons learned from cybersecurity incidents, the third-party assessment of CAST, and other cybersecurity incident response protocols; and (3) defining S&R's responsibilities in the cybersecurity incident response process and how the cybersecurity incident response and supervision processes interact. As part of this project, S&R plans to update the playbook. Interviewees stated that S&R expects to issue the updated playbook in 2023.

In addition, the Board and CAST have initiated a project to improve the data quality of cybersecurity incidents entered into the CER and to overhaul the user interface and experience of the system. The

[9] The severity of a cybersecurity incident is assessed using a six-point scale ranging from level 0, or *baseline*, which is an unsubstantiated or inconsequential event, to level 5, or *emergency*. Each cybersecurity incident is assigned two severity ratings—one assessing its severity to the financial institution and one assessing its severity to the financial sector. Incidents with an institution severity rating of level 5 pose a severe risk of imminent insolvency to the supervised entity. Incidents with a sector severity rating of level 5 pose an imminent threat to the provision of wide-scale critical infrastructure services, to national government stability, or to the lives of U.S. persons.

[10] We did not assess the roles of these groups in the cybersecurity incident response process.

[11] The playbook outlines procedures for communicating with other federal financial regulatory agencies. We did not assess the roles of these other federal agencies individually or collectively in the cybersecurity incident response process.

Board and CAST plan to complete the key components of this effort in February 2024, although continued refinements to the system are expected to be completed after that date.

Finding 1: The Board Can Update Guidance to Clarify the Mission and Governance Structure of the Cybersecurity Incident Response Process

We found that some staff involved in the cybersecurity incident response process do not clearly understand SORP's or OR's roles and responsibilities in overseeing the process. According to the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. As part of this process, management should assign responsibilities to discrete units to enable the organization to operate in an efficient and effective manner and consider how units interact to fulfill their overall responsibilities. We attribute the lack of understanding regarding SORP's and OR's roles and responsibilities in overseeing the cybersecurity incident response process to guidance documents that do not clearly describe the mission or the governance structure of the process. A clearly defined mission and governance structure for the cybersecurity incident response process should help guide the efforts of the parties involved and help enhance the effectiveness of the Board and Reserve Banks' response to cybersecurity incidents.

Some Staff Do Not Clearly Understand the Roles and Responsibilities of SORP or OR in the Cybersecurity Incident Response Process

We found that some staff involved in the cybersecurity incident response process do not clearly understand SORP's or OR's oversight roles and responsibilities for the process. Specifically, interviewees identified a need to clarify the roles and responsibilities of SORP and OR in their joint oversight of the process and stated that it is unclear who is ultimately responsible for the process, including who has the final authority in decisionmaking. For instance, an interviewee stated that the playbook does not clearly define who ultimately reviews and approves the communication processes.

According to GAO's *Standards for Internal Control in the Federal Government*, management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. As part of this process, management should assign responsibilities to discrete units to enable the organization to operate in an efficient and effective manner and consider how units interact to fulfill their overall responsibilities.

The Board Can Clarify the Mission of the Cybersecurity Incident Response Process and Its Governance Structure

We attribute the lack of understanding regarding SORP's and OR's roles and responsibilities to guidance documents that do not clearly describe the cybersecurity incident response process's mission or governance structure. SORP, OR, and CAST staff frequently identified the playbook as the primary governing document for the process; however, the playbook does not clearly define the purpose of the process or its current governance structure.

In our review of documentation related to the cybersecurity incident response process, we identified references to mission statements, but those statements do not clearly articulate the purpose of the process. Specifically, we identified two documents that included a mission statement—OR's oversight plan for CAST and the project charter for OR and SORP's ongoing review of the cybersecurity incident response process. Both documents state that the objective of the cybersecurity incident response process is to best position S&R to make decisions related to the safety and soundness of the banking and financial system by coordinating with stakeholders, disseminating relevant information, and assessing risks to supervised entities. However, interviewees noted that supervised entities conduct incident management, while the Board communicates about the cybersecurity incident with other stakeholders.

Further, multiple interviewees also stated there were opportunities to refine and clarify the mission of the cybersecurity incident response process. In addition, one interviewee stated that the Board not defining the mission of the incident response process can affect S&R's coordination with other Board divisions and the Board's external coordination and communication with other federal regulators. The interviewee stated that some of the gaps in the Board's capabilities in this area could be addressed through developing better internal procedures, noting that sharing information with other Board divisions and other regulators in a timely manner is important because it can help prevent further damage to other institutions or the financial sector.

We acknowledge that S&R has taken steps to define the mission of the cybersecurity incident response process in OR's oversight plan for CAST and the project charter for SORP and OR's ongoing review of the cybersecurity incident response process; however, we believe that the process's mission should be articulated in the playbook as it is the primary governing document of the incident response process and is accessible to the key stakeholders involved in the process. Further, we believe that S&R should assess whether the mission statement outlined in the two documents described above continues to align with its vision for the process or whether there are opportunities to further refine the mission of the incident response process.

We also found that some of the guidance documents related to the cybersecurity incident response process do not reflect the current governance structure of the process. For instance, the playbook states that SORP will oversee and coordinate the process and oversee CAST's assessment of the severity of a cybersecurity incident; in addition, CAST's operating procedures, which were last updated in March 2021, state that SORP has oversight of CAST. Neither document has been updated to reflect that SORP and OR share oversight of CAST and the cybersecurity incident response process.

In addition, we found that one of the guidance documents related to the cybersecurity incident response process does not clearly describe the process's governance structure. Specifically, OR's CAST oversight plan, which according to an S&R official was developed jointly by SORP and OR, does not clearly define the role of SORP in overseeing CAST. While the oversight plan briefly mentions SORP staff, it does not describe how oversight responsibilities will be shared between the two groups or how decisionmaking authority will be exercised.

We believe that clearly defining the mission and governance structure—the purpose of the cybersecurity incident response process and the roles and responsibilities of the groups overseeing it—will increase the effectiveness of the Board and Reserve Banks' response when a cybersecurity incident occurs at a supervised institution.

Recommendations

We recommend that the director of S&R

1. Update the playbook to clarify the mission and reflect the governance structure of the cybersecurity incident response process. As part of this effort, consider whether the current mission statement aligns with the Board's vision for this process.
2. Update the oversight plan for CAST to clearly describe the governance structure of the cybersecurity incident response process, including
    a. the roles and responsibilities of SORP and OR in overseeing the cybersecurity incident response process.
    b. how decisionmaking authority will be exercised.
3. Update CAST's operating procedures to reflect the governance structure.

Management Response

In its response to our draft report, the Board concurs with our recommendations and states that it believes that the recommendations related to mission, governance structure, and alignment to the Board's vision are best addressed by implementing a governance framework. The Board notes that it will document its governance structures in the framework, providing visibility into the incident response processes across S&R. In addition, the Board states that the project charter for SORP and OR's ongoing review of the cybersecurity incident response process is being updated to include the proposed governance framework and will be submitted for approval in the third quarter of 2023.

To address recommendation 1, the Board states that the playbook is in the process of being updated and that it plans to publish the updated playbook by the end of the fourth quarter of 2023.

To address recommendation 2, the Board states that by the end of the third quarter of 2023, it will finalize service-level expectations for CAST. The Board notes that the service-level expectations will replace the oversight plan for CAST and will include roles and responsibilities and decisionmaking authority that are aligned with the governance framework and the playbook.

To address recommendation 3, the Board states that as part of the service-level expectations that are being finalized, CAST will be expected to update its operating procedures and that OR will assess the updates by the end of the first quarter of 2024.

OIG Comment

The actions described by the Board appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 2: The Board Can Enhance Guidance and Training on the Cybersecurity Incident Response Process

We found that the Board and Reserve Banks' responses to cybersecurity incidents have not consistently followed the cybersecurity incident response process prescribed in guidance. In addition, multiple interviewees indicated that some stakeholders are unclear on their roles and responsibilities and that training would be beneficial. According to GAO's *Standards for Internal Control in the Federal Government*, management should document responsibilities for processes in its policies and, if there is a significant change in a process, review this process in a timely manner after the change to determine that activities are designed and implemented appropriately. Further, these standards note the importance of training in helping an organization to achieve its objectives. We attribute the inconsistencies and stakeholders' lack of clarity regarding their roles and responsibilities to unclear and outdated guidance on the cybersecurity incident response process. Clearly documenting the cybersecurity incident response process and the roles and responsibilities of key stakeholders, and providing training to staff on these topics, will enhance the effectiveness of the Board and Reserve Banks' response when a cybersecurity incident occurs at a supervised institution.

Board and Reserve Bank Cybersecurity Incident Responses Have Not Been Consistent With Guidance

We found that the Board and Reserve Banks have not been consistently following the cybersecurity incident response process prescribed in guidance when responding to cybersecurity incidents. Specifically, we identified three examples of those types of inconsistencies:

- Severity ratings: The playbook outlines procedures that differ based on the severity rating of the incident, but it does not state which severity rating—institution severity or sector severity—determines which procedure should be followed. A CAST interviewee stated that the procedures outlined in the playbook are based on the sector severity rating; however, interviewees stated that CAST adjusts the sector severity rating throughout the life cycle of a cybersecurity incident as a financial institution takes action to mitigate the risk. In addition, the playbook states that CAST assigns the severity rating, but it does not specify which rating. According to interviewees, CPCs assign the institution severity rating.
- AAR: The playbook states that AARs shall be completed for cybersecurity incidents with a severity rating of *medium* or higher; however, we found that the Board and Reserve Banks did not complete an AAR for a cybersecurity incident with a sector severity rating of *medium*. In addition, the playbook contains conflicting information regarding whether SORP or CAST is responsible for completing AARs. An interviewee stated that this responsibility has shifted to CAST because of resource constraints within SORP.

- Escalation to Board members: The playbook directs SORP to provide written briefings to Board members for cybersecurity incidents with a severity rating of *high* or *severe*; however, we found instances in which Board members were provided written briefings on cybersecurity incidents with a sector severity rating of *low*. We believe the Board can benefit from defining the circumstances that warrant informing Board members of a cybersecurity incident with a severity rating other than high or severe.

Some Stakeholders Indicated That Additional Training Would Be Beneficial

The Board has previously held trainings and exercises related to the cybersecurity incident response process. In 2022, the Board and CAST held trainings for examination staff on how to use the CER and on the Notification Rule requirements. The Board also conducted table-top exercises[12] with CPCs and Reserve Bank management in the community banking organization and regional banking organization portfolios in 2022 as part of its project to enhance the cybersecurity incident response process.[13]

However, multiple interviewees indicated that some stakeholders in the cybersecurity incident response process are unclear on their roles and responsibilities and that additional training would be beneficial. For example, one interviewee stated that examiners in the community banking organization and regional banking organization portfolios do not always understand the incident response process and may lack cybersecurity knowledge. Another interviewee noted that it may take additional time to initiate the process with groups who are not familiar with responding to cybersecurity incidents. In addition, interviewees stated that training would be beneficial for staff in SORP, citing staff turnover and the need for staff to have specific skills related to cybersecurity incident response.

The Board Can Update and Enhance Guidance on the Cybersecurity Incident Response Process

According to GAO's *Standards for Internal Control in the Federal Government*, management should document responsibilities for processes in its policies and, if there is a significant change in a process, review this process in a timely manner after the change to determine whether activities have been designed and implemented appropriately. Further, documenting processes furthers organizational knowledge retention. In addition, these standards note the importance of training in helping an organization to achieve its objectives.

The playbook states that it should be reviewed at least annually and that it will be regularly updated to accurately reflect changes to participants, tools, and techniques; however, the playbook has not been updated since October 2020. Since that time, the cybersecurity incident response process has undergone significant changes, including changes resulting from the Notification Rule. For example, financial

[12] Table-top exercises simulate high severity incidents and help enhance incident preparedness by familiarizing decisionmakers with the procedures in the playbook.

[13] The community banking organization portfolio includes institutions with less than $10 billion in total consolidated assets. The regional banking organization portfolio includes institutions with $10 billion to $100 billion in total consolidated assets.

institutions are subject to new reporting requirements under the Notification Rule, and CAST is responsible for entering cybersecurity incidents reported under the Notification Rule into the CER.

We attribute the inconsistencies we found in the responses to cybersecurity incidents and stakeholders' lack of clarity regarding their roles and responsibilities in the cybersecurity incident response process to the playbook and its implementing guidance being unclear and outdated. For example, the playbook outlines procedures that differ based on the severity rating of the incident and notes that CAST will periodically revisit the severity rating of a cybersecurity incident as new facts emerge and that SORP will approve the escalation or de-escalation of a severity rating. However, the playbook does not define (1) which severity rating—institution severity or sector severity—it is referring to, (2) the differences in the processes for assigning and updating each severity rating, or (3) the criteria for changing a severity rating. Further, the playbook does not clearly describe how changes to the severity rating affect which procedures staff should follow, which may create confusion because those procedures are based on the severity rating.

In other instances, Board and Reserve Bank staff indicated that the cybersecurity incident response process described in the playbook may not reflect the current practices or needs of stakeholders. For example, a CAST member stated that an AAR was not completed for a cybersecurity incident that met the threshold outlined in the playbook because the vulnerability related to this incident was not widespread. In another instance, a Board official stated that S&R sometimes informs Board members of lower severity cybersecurity incidents if the incident is expected to receive media attention. We acknowledge that there may be circumstances in which Board members may need to be informed of lower severity cybersecurity incidents and that the process outlined in the playbook may no longer meet the needs of stakeholders. Thus, we believe that reassessing these aspects of the process and updating the playbook to reflect current practices will provide stakeholders with a clear understanding of the process to follow when responding to cybersecurity incidents.

Further, the Board's internal guidance to implement the playbook is also outdated. Like the playbook, this guidance has not been updated to reflect the changes to the cybersecurity incident response process resulting from the Notification Rule. In addition, the guidance does not mention OR despite its role in the process.

As previously noted, S&R plans to update the playbook as part of its project to enhance the cybersecurity incident response process. For example, S&R conducted a gap assessment of the existing playbook and plans to better define the roles and responsibilities throughout the life cycle of an incident and clarify who is responsible for completing AARs and when they will be completed. While we acknowledge that S&R plans to address some of the areas we identified as part of its playbook update, we believe that there are additional areas in which the process can be improved.

Clearly documenting the cybersecurity incident response process and the roles and responsibilities of key stakeholders will enhance the effectiveness of the Board and Reserve Banks' response when a cybersecurity incident occurs at a supervised institution. Further, providing training to key stakeholders in the process will ensure that they understand their responsibilities and can respond when a cybersecurity incident occurs.

Recommendations

We recommend that the director of S&R

4. Update the playbook to
    a. reflect the requirements for financial institutions to report cybersecurity incidents under the Notification Rule and any associated changes to the cybersecurity incident response process or the roles and responsibilities of stakeholders.
    b. clarify whether references to the severity rating are referring to the institution severity rating or sector severity rating, the process and criteria for changing a severity rating, and how changes to the severity rating affect the cybersecurity incident response procedures staff should follow.
    c. clarify the requirement for completing an AAR after a cybersecurity incident and the party responsible for completing it.
    d. clarify the circumstances that warrant informing Board members of a cybersecurity incident.
5. Update the Board's December 2018 playbook implementing guidance to reflect
    a. the updates made to the playbook as part of recommendation 4.
    b. the role of OR in the cybersecurity incident response process.
    c. the governance structure of the cybersecurity incident response process.
6. Require that key stakeholders in the cybersecurity incident response process complete training or other exercises on their roles and responsibilities in the process once the updates to the playbook and its implementing guidance have been completed.

Management Response

In its response to our draft report, the Board concurs with our recommendations.

To address recommendation 4, the Board states that by the end of the fourth quarter of 2023, it will update the playbook to reflect the requirements of the Notification Rule and update the roles and responsibilities of stakeholders. The Board notes that the playbook updates will also clarify and address the issues we cited regarding severity ratings, AARs, and circumstances that warrant informing Board members.

To address recommendation 5, the Board states that it will issue updated guidance in the first quarter of 2024 to reflect the significant changes to the playbook, the role of OR in the cybersecurity incident response process, and the governance structure.

To address recommendation 6, the Board states that it plans to complete training for key stakeholders in the cybersecurity incident response process by the end of the fourth quarter of 2024.

OIG Comment

The actions described by the Board appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Appendix A: Methodology

We initiated this evaluation to assess the Board and Reserve Banks' cybersecurity incident response process for supervised institutions. During our scoping phase, we developed an understanding of the Board and Reserve Banks' cybersecurity incident response process. Specifically, we interviewed responsible Board and Reserve Bank officials and staff and reviewed policies and procedures related to the cybersecurity incident response process for supervised institutions. We also reviewed CER data from January 1, 2021, through September 30, 2022. In addition, we reviewed documents related to the third-party assessment of CAST, S&R's project to enhance the cybersecurity incident response process, and CAST's project to enhance the CER.

We conducted our scoping phase from August 2022 through April 2023 in accordance with the *Quality Standards for Inspection and Evaluation*, issued in December 2020 by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B: Management Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

June 14, 2023

Mr. Michael VanHuysen
Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of The Federal Reserve System
Washington, DC 20551

Dear Mr. VanHuysen,

Thank you for the report, *Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institution*, prepared by the Office of Inspector General (OIG). We appreciate the effort that the OIG has put into this report and the recommendations provided for enhancing our cybersecurity incident response process.

The report addresses two areas of the incident response process for enhancement: clarifying the mission and governance structure of the cybersecurity incident response process and providing guidance and training on the process. The Division of Supervision and Regulation (S&R) agrees with the conclusions and recommendations.

The Board Can Update Guidance to Clarify the Mission and Governance Structure of the Cybersecurity Incident Response Process

S&R believes that the recommendations related to mission, governance structure and alignment to the "Board's vision" are best addressed by implementing a governance framework. The framework will provide visibility of incident response processes across S&R and document our governance structures. The project charter for Systems and Operational Resiliency Policy (SORP) and Operational Resilience's (OR) ongoing review of the cybersecurity incident response process is currently being updated. It will be submitted for approval in 3Q 2023 and will include the proposed governance framework.

Recommendation 1: Update the playbook to clarify the mission and reflect the governance structure of the cybersecurity incident response process. As part of this effort, consider whether the current mission statement aligns with the Board's vision for this process.

The playbook is in the process of being updated. S&R is currently reviewing the update and the project is on-target to complete the updates and publish the playbook by the end of 4Q 2023.

Recommendation 2: Update the oversight plan for CAST to clearly describe the governance structure of the cybersecurity incident response process, including the roles and responsibilities of SORP and OR in overseeing the cybersecurity incident response process as well as how decisionmaking authority will be exercised.

The formal CAST service level expectations (SLE) document is in the process of being finalized by the end of 3Q 2023. It will include roles and responsibilities and decision-making authority that are aligned with the governance framework and the playbook. This SLE will replace the current CAST 2022-2023 oversight plan.

Recommendation 3: Update CAST's operating procedures to reflect the governance structure.

The expectations for CAST to update their operating procedures are part of the SLE and will be included in the final agreement. CAST will update their operating procedures and the OR Program will assess the update by the end of 1Q 2024.

The Board Can Enhance Guidance and Training on the Cybersecurity Incident Response Process

Recommendation 4: Update the playbook to

a. *reflect the requirements for financial institutions to report cybersecurity incidents under the Notification Rule and any associated changes to the cybersecurity incident response process or the roles and responsibilities of stakeholders.*
b. *clarify whether references to the severity rating are referring to the institution severity rating or sector severity rating, the process and criteria for changing a severity rating, and how changes to the severity rating affect the cybersecurity incident response procedures staff should follow.*
c. *clarify the requirement for completing an AAR after a cybersecurity incident and the party responsible for completing it.*
d. *clarify the circumstances that warrant informing Board members of a cybersecurity incident.*

S&R is currently updating the playbook to reflect the requirements of the Notification Rule and update the roles and responsibilities of stakeholders. The playbook updates will also clarify and address the issues cited by the OIG on severity ratings, AARs, and circumstances that warrant informing Board members. S&R is currently reviewing the draft update and the project is on-target to complete the finalized playbook by the end of 4Q23.

Recommendation 5: Update the Board's December 2018 playbook implementing guidance to reflect

a. *the updates made to the playbook as part of recommendation 4.*
b. *the role of OR in the cybersecurity incident response process.*
c. *the governance structure of the cybersecurity incident response process.*

S&R will issue an updated Advisory Letter (also known as an AD Letter) to reflect the significant changes to the playbook, the role of OR in the cybersecurity incident response process, and the governance structure. As previously noted, S&R believes observations on the governance structure are best served by implementing a governance framework to provide visibility of response processes across S&R, practice exercising the response processes, and document our governance structures. The governance framework is reflected in an update to the project charter noted in the observation details of the report. The AD letter will be issued in 1Q 2024 after the finalization/approval of the playbook.

Recommendation 6: Require that key stakeholders in the cybersecurity incident response process complete training or other exercises on their roles and responsibilities in the process once the updates to the playbook and its implementing guidance have been completed.

The planning for training and exercises will occur upon completion of the updated playbook and is included in the success factors of the updated project charter. We plan to conduct training for key stakeholders in the cybersecurity incident response process by the end of 4Q 2024.

We value your objective and independent viewpoints and appreciate the professionalism demonstrated by all OIG personnel throughout this audit and your efforts to understand our process. We look forward to continuing to work with your office in the future.

Regards,

MICHAEL GIBSON Digitally signed by MICHAEL GIBSON
Date: 2023.06.13 16:01:14 -04'00'

Michael S. Gibson
Director
Division of Supervision and Regulation

Abbreviations

AAR	after action reviews
CAST	Cybersecurity Analytics Support Team
CER	Cyber Event Repository
CPC	central point of contact
GAO	U.S. Government Accountability Office
OR	Operational Resilience
S&R	Division of Supervision and Regulation
SORP	Systems and Operational Resiliency Policy

Report Contributors

Lindsay Taylor, Project Lead and Senior Auditor
Kamry Bennett, Auditor
Carissa Haynes, Auditor
Andrew Luckman, Forensic Auditor
Tessah Sperry, Forensic Auditor
Tina Vuong, Auditor
Victor Calderon, OIG Manager for Data Analytics
Michael Zeitler, OIG Manager, Supervision and Regulation
Laura Shakarji, Senior OIG Manager for Supervision and Regulation
Cynthia Gray, Deputy Associate Inspector General for Audits and Evaluations
Michael VanHuysen, Associate Inspector General for Audits and Evaluations

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I 2322
Washington, DC 20551

Phone: 800 827 3340
Fax: 202 973 5044