Evaluation Report
2020-SR-B-019
September 30, 2020

Board of Governors of the Federal Reserve System

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

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

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

Executive Summary, 2020-SR-B-019, September 30, 2020

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

Findings

The Board of Governors of the Federal Reserve System's approach to cybersecurity supervision of Large Institution Supervision Coordinating Committee (LISCC) firms continues to evolve and can be enhanced. We determined that the Board can strengthen its governance of LISCC firm cybersecurity supervision. Over the past several years, the Board's Division of Supervision and Regulation (S&R) has undergone several structural changes affecting its governance of the cybersecurity supervision for LISCC firms. These structural changes have created a need to define the roles and responsibilities of the groups that are currently involved in LISCC cybersecurity supervision and planning. Additionally, the Board can better define how cybersecurity supervisory activities inform the governance and controls ratings of LISCC firms. Clarifying how weaknesses or deficiencies identified during cybersecurity supervision activities factor into these ratings can help the LISCC program better communicate its assessment regarding firms' cybersecurity posture.

Further, the LISCC program can enhance its approach to cybersecurity training. In addition, some cybersecurity examiners have difficulty obtaining training. The inability of cybersecurity examiners to keep their skills updated could affect their readiness to examine emerging cybersecurity risk areas and can adversely affect retention and recruitment. Finally, examiners would benefit from additional guidance and training on reporting cybersecurity incidents in the Federal Reserve System's designated repository. Absent clear guidance and training, users may not be consistently entering cybersecurity events into the repository, increasing the likelihood that the System may not be effectively and timely synthesizing information on cybersecurity incidents.

Recommendations

Our report contains recommendations designed to enhance the effectiveness of the Board's cybersecurity supervision of LISCC firms. In its response to our draft report, the Board concurs with our recommendations and outlines actions that have been or will be taken to address our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We conducted this evaluation to assess the effectiveness of the Board's and the Federal Reserve Banks' cybersecurity supervision approach for LISCC firms. The scope of our evaluation included applicable laws, regulations, policies, procedures, and agency practices related to the cybersecurity supervision of LISCC firms.

Background

S&R is responsible for leading the System's supervisory activities. The LISCC is chaired by the director of S&R and is responsible for overseeing the supervision of the largest, most systemically important financial institutions under the Board's purview.

Cybersecurity risks present significant and dynamic challenges to LISCC firms. Board and Reserve Bank staff supervise LISCC firms through a combination of horizontal examinations, firm-specific idiosyncratic examinations, and monitoring activities. The governance and controls core assessment program, one of four LISCC core assessment programs, is responsible for overseeing the supervision of LISCC firm information technology and cybersecurity risks, among other areas. The LISCC program's supervisory work culminates in an annual integrated assessment letter for each firm, which highlights key themes and supervisory concerns. It also culminates in annual ratings for three core assessment areas, including a governance and controls rating, under the Board's large financial institution rating system.

Recommendations, 2020-SR-B-019, September 30, 2020

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

Finding 1: Governance of LISCC Firm Cybersecurity Supervision Can Be Strengthened

Number	Recommendation	Responsible office
1	Formalize the governance of LISCC cybersecurity supervision to clarify roles, responsibilities, and authorities of the LISCC program and other groups that may play a role in LISCC cybersecurity supervision matters, such as the BTR section.	Division of Supervision and Regulation
2	Update the G&C operating manual to reflect the position of the cybersecurity horizontal team within the LISCC program and establish a clear objective for that team.	Division of Supervision and Regulation
3	Develop a plan to ensure that the LISCC program, in consultation with the BTR section, incorporates interagency coordinated reviews in its supervisory planning processes for LISCC firms.	Division of Supervision and Regulation
4	Develop a plan to define how cybersecurity information from cross-portfolio groups, such as CAST and the BTR section, contributes to the planning process for LISCC cybersecurity supervision activities.	Division of Supervision and Regulation

Finding 2: The LISCC Program Can Better Define How to Factor the Results of Cybersecurity Supervision Activities Into Firm G&C Ratings

Number	Recommendation	Responsible office
5	Define the steps for considering the results of cybersecurity supervisory activities when determining LISCC firms' G&C rating within the new LFI rating system.	Division of Supervision and Regulation

Finding 3: The LISCC Program Can Enhance Its Approach to Cybersecurity Training

Number	Recommendation	Responsible office
6	Develop a structured cybersecurity training plan for cybersecurity examiners. As part of the plan, define expectations for skill sets and for continuing education, such as training related to emerging risks.	Division of Supervision and Regulation
7	Require that relevant examiners complete cybersecurity training in a manner consistent with the plan to address recommendation 6.	Division of Supervision and Regulation

Finding 4: The Board Can Enhance Guidance and Training on Reporting Cybersecurity Events

Number	Recommendation	Responsible office
8	Update the Board's April 2018 guidance on the CER to clearly define the types of cybersecurity events that should be entered into the system.	Division of Supervision and Regulation
9	Develop instructions and training on using the CER, and issue guidance that requires CPCs, or their designees, to complete this training.	Division of Supervision and Regulation
10	Update the cybersecurity incident playbook to reflect S&R's current organizational structure.	Division of Supervision and Regulation

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

MEMORANDUM

DATE: September 30, 2020

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 2020-SR-B-019: *The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced*

We have completed our report on the subject evaluation. We conducted this evaluation to assess the effectiveness of the Board of Governors of the Federal Reserve System's and the Federal Reserve Banks' cybersecurity supervision approach for Large Institution Supervision Coordinating Committee firms.

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 the Reserve Banks during our evaluation. Please contact me if you would like to discuss this report or any related issues.

cc: Jennifer Burns
Arthur Lindo
Lisa Ryu
Nida Davis
Michael Hsu
John Beebe
Kevin Bertsch
Ray Diggs
Tracy Basinger
James T. Nolan
Kevin Stiroh
Lisa White
Danny Brando
Jason Tarnowski

Danielle Vacarr
Ryan Lordos
Jennifer Herring
Kimberly Perteet
Melissa Vanouse
Tiffany Wilkins
Haley Gibson
Ricardo A. Aguilera
Cheryl Patterson

Contents

Introduction **9**

Objective 9

Background 9

The Board's Role in Supervision 9

LISCC Program Structure and Supervision 9

Cybersecurity and LISCC Firms 10

The LISCC Program's Cybersecurity Supervision Approach 11

Finding 1: Governance of LISCC Firm Cybersecurity Supervision Can Be Strengthened **13**

S&R Has Undergone Several Structural Changes Affecting Its Governance of LISCC Firm Cybersecurity Supervision 13

Structural Changes Have Created a Need to Clarify Roles and Responsibilities Pertaining to LISCC Firm Cybersecurity Supervision and Planning 14

Reporting Line and Objective for the Cybersecurity Horizontal Team 15

Approach to Coordinating Interagency Cybersecurity Examinations 15

Role of Certain Cross-Portfolio Groups in Cybersecurity Supervision Planning 15

Conclusion 17

Recommendations 17

Management Response 17

OIG Comment 18

Finding 2: The LISCC Program Can Better Define How to Factor the Results of Cybersecurity Supervision Activities Into Firm G&C Ratings **19**

The LISCC Program Has Not Defined Expectations for How Its Cybersecurity Supervisory Activities Inform the G&C Rating of the Newly Established LFI Rating System 19

Recommendation 20

Management Response 20

OIG Comment 20

Finding 3: The LISCC Program Can Enhance Its Approach to Cybersecurity Training **21**

Some Cybersecurity Examiners Have Difficulty Obtaining Training 21

Training Difficulties Impede Cybersecurity Examiner Development, Retention, and Hiring Efforts 22

Recommendations 23
Management Response 23
OIG Comment 23

Finding 4: The Board Can Enhance Guidance and Training on Reporting Cybersecurity Events 24

Guidance for the CER Is Fragmented and Unclear 24
Some Reserve Bank Examiners Are Unclear on How to Use the CER 26
CER Users Have Limited Access to Training and Guidance 27
The CER Contains Few LISCC Firm Incidents and Missing Information 27
Recommendations 28
Management Response 28
OIG Comment 28

Appendix A: Scope and Methodology 29

Appendix B: Management Response 31

Abbreviations 35

Introduction

Objective

Our objective for this evaluation was to assess the effectiveness of the Board of Governors of the Federal Reserve System's and the Federal Reserve Banks' cybersecurity supervision approach for Large Institution Supervision Coordinating Committee (LISCC) firms.[1] The scope of our evaluation included applicable laws, regulations, policies, procedures, and agency practices related to the cybersecurity supervision of LISCC firms. We reviewed the cybersecurity supervision activities executed by the LISCC program and the four Reserve Banks with LISCC firms in their Districts—the Federal Reserve Banks of Boston, New York, Richmond, and San Francisco. Our scope did not include firms in the community banking organization, regional banking organization, or large and foreign banking organization portfolios, nor did our scope include supervisory activities unrelated to cybersecurity. Appendix A describes our scope and methodology in greater detail.

Background

The Board's 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 laws and regulations. The Board's Division of Supervision and Regulation (S&R) is responsible for leading the Federal Reserve System's supervisory activities. S&R organizes its oversight activities into supervisory portfolios that are generally based on institutions' total asset size.

The LISCC portfolio includes the largest, most systemically important domestic and foreign financial institutions supervised by the Board. The LISCC is a System committee that is chaired by the director of S&R and comprises senior officers representing various functions at the Board and the Reserve Banks. The LISCC Operating Committee, in consultation with the LISCC, is responsible for executing the LISCC program. As of June 2020, the LISCC portfolio comprises 11 firms—8 domestic and 3 foreign.[2]

LISCC Program Structure and Supervision

In early 2018, the Board reorganized the LISCC program to include four core assessment programs—capital, resolution and recovery, liquidity, and governance and controls (G&C). In addition, the monitoring and analysis program (MAP) supports those core assessment programs by identifying emerging risks, trends, and practices that may affect individual firm resiliency or the resiliency of the LISCC portfolio as a

[1] The responsibility for the supervision of LISCC firms rests with the LISCC Operating Committee and the director of the Division of Supervision and Regulation (S&R), not the Reserve Banks. As a result, we directed our findings and recommendations to the director of S&R.

[2] When we initiated this evaluation, the LISCC portfolio comprised 12 firms—8 domestic and 4 foreign. In March 2020, the LISCC program removed one of the foreign firms from the LISCC portfolio.

whole. A steering committee comprising Board and Reserve Bank officers leads each of the core assessment programs and the MAP.

In addition to LISCC staff assigned to the core assessment programs and the MAP, the LISCC program includes 11 dedicated supervisory teams (DSTs) comprising Reserve Bank officers and examiners assigned to supervise the respective LISCC firms on an ongoing basis (figure 1).

Figure 1. LISCC Program Organizational Chart

Source: Generated by the OIG based on LISCC program documentation.

Board and Reserve Bank staff execute LISCC program supervision through a combination of horizontal examinations, firm-specific idiosyncratic examinations, and monitoring activities designed to assess both the resiliency of an individual firm and of the LISCC portfolio as a whole.

The LISCC program's supervisory work culminates in an annual integrated assessment letter for each firm, which informs the firm's senior management and board of directors of the findings from the core assessment programs and highlights key themes and supervisory concerns. It also culminates in annual component ratings for three of the four core assessment areas, including a G&C component rating, under the System's large financial institution (LFI) rating system.[3]

Cybersecurity and LISCC Firms

Cybersecurity is the process of protecting networks, devices, and data from unauthorized access and ensuring the confidentiality, integrity, and availability of information. Over the past several years, cybersecurity threats have evolved and increased significantly, occurring on a more frequent basis and with greater sophistication. As financial institutions' dependence on technology for critical operations, new products and services, and service delivery to consumers and businesses increases, the threats to this technology have become more prevalent.

[3] Under the LFI rating system, which was implemented in February 2019, there are three component ratings—G&C, capital planning and positions, and liquidity risk management and positions. At least annually, the LISCC program assigns LISCC firms one of the following four ratings for each of the three components: *broadly meets expectations*, *conditionally meets expectations*, *deficient-1*, or *deficient-2*. The LFI rating system does not include an overall composite rating.

Cybersecurity is an area of significant focus for firms and federal financial regulators and will likely continue to be an area of concern in the future. In its past five annual reports to Congress, the Financial Stability Oversight Council (FSOC) has identified cybersecurity as an area of major concern for companies and governments around the world.[4] Similarly, in a 2018 speech, the Board's vice chair for supervision stated that the dynamic and highly sophisticated nature of cybersecurity risks requires that the public and private sectors collaborate to identify and manage those risks.[5] The Board's chair also noted in a 2019 television interview that cybersecurity risk is constantly evolving and that ensuring financial institutions are resilient to cyberattacks has become a major focus area for the Federal Reserve.[6]

The supervision of financial institutions, including LISCC firms, is one of the Board's principal methods to ensure that the nation's financial system operates in a safe and sound manner. A cybersecurity breach caused by the interference, degradation, or unauthorized alteration of information and systems that support LISCC firms' critical functions can expose these institutions to operational, reputational, and financial risks as well as potentially disrupt the smooth functioning of certain financial markets or activities. A cybersecurity event with severe negative consequences for a LISCC firm could affect the U.S. economy and financial stability, given the systemic importance of these institutions and the services they provide in support of certain financial markets.

The LISCC Program's Cybersecurity Supervision Approach

The LISCC G&C core assessment program is responsible for overseeing the supervision of LISCC firm information technology (IT) and cybersecurity risks, among other areas. The G&C program's objectives are to assess the effectiveness of the oversight provided by LISCC firms' boards of directors, the core business lines' risk management, and the firms' independent risk management and controls. The LISCC program's approach to evaluating firms' cybersecurity processes consists primarily of conducting horizontal examinations, supplemented by idiosyncratic supervisory activities.

Since 2015, the LISCC program has initiated four cybersecurity horizontal examinations (figure 2). Each horizontal examination addresses one topical area pertaining to cybersecurity risks and is executed by members of a horizontal team. The LISCC program's cybersecurity horizontal examinations have generally covered the elements of the National Institute of Standards and Technology's Cybersecurity Framework, such as identifying and responding to cybersecurity threats.[7] That framework—which is widely used by the financial industry and across critical infrastructure sectors—describes standards, guidelines, and best practices to manage cybersecurity risk.

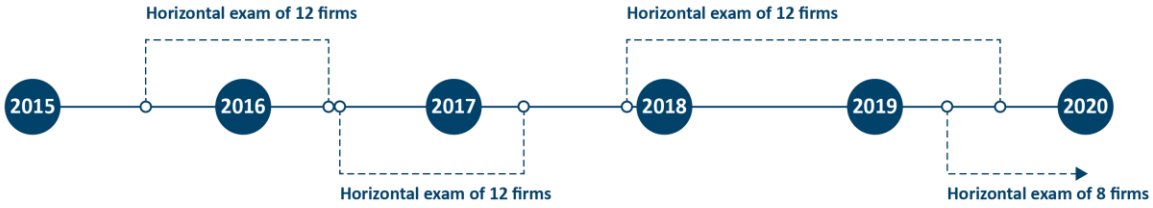
[4] Established under the Dodd-Frank Wall Street Reform and Consumer Protection Act, FSOC is authorized to identify risks to the financial stability of the United States, promote market discipline, and respond to emerging risks to the stability of the U.S. financial system.

[5] The vice chair provided his thoughts on the Board's cybersecurity supervision in a speech at the Financial Services Roundtable 2018 Spring Conference on February 26, 2018.

[6] The chair appeared on the CBS News show *60 Minutes* on March 10, 2019.

[7] The elements of the National Institute of Standards and Technology's Cybersecurity Framework are *identify*, *protect*, *detect*, *respond*, and *recover*.

Figure 2. LISCC Program Cybersecurity Horizontal Examinations, 2015–March 2020



Source: OIG analysis of LISCC program examination documentation.

To supplement the horizontal examinations, the LISCC program conducts some firm-specific or idiosyncratic cybersecurity supervisory activities. Such activities can include target examinations, MAP in-depth reviews,[8] and activities to follow up on Matters Requiring Attention or Matters Requiring Immediate Attention. According to a LISCC official, the LISCC program may initiate these idiosyncratic cybersecurity activities if it identifies issues that warrant further inquiry or if the Board is the primary federal regulator of the firm, among other factors. These supervisory activities provide additional insight into specific aspects of a firm's cybersecurity program and help examiners to determine whether the firms have adequately addressed the supervisory issues identified in prior examinations. From 2016 to 2019, the LISCC program completed from one to seven idiosyncratic examinations with cybersecurity-related components for some LISCC firms, and no such examinations for other LISCC firms.[9]

[8] MAP in-depth reviews are discrete investigations of narrowly defined topics that may constitute an emerging risk or issue.

[9] There were 12 firms in the LISCC portfolio from 2016 to March 2020.

Finding 1: Governance of LISCC Firm Cybersecurity Supervision Can Be Strengthened

The Board can strengthen its governance of LISCC firm cybersecurity supervision. *Organizational governance* involves processes and structures for decisionmaking, accountability, controls, and behaviors designed to accomplish organizational objectives. Over the past several years, S&R has undergone several structural changes affecting its governance of cybersecurity supervision for LISCC firms. In 2015, S&R launched the Cybersecurity Program Group (CPG) within the division's policy function to improve the System's oversight of cybersecurity. In 2019, as part of a reorganization of the division, S&R established the Business Technology Risk (BTR) section in the division's supervision function to develop and coordinate an integrated IT supervisory program. S&R later dissolved the CPG, stating that many of its responsibilities had shifted to the BTR section and another group within the policy function. In the midst of these changes, the LISCC program also implemented a reorganization that consolidated the supervision of nonfinancial risks, including cybersecurity, under the G&C program. These significant structural changes have created a need to define the roles and responsibilities of the groups that are currently involved in LISCC cybersecurity supervision and planning and how they should coordinate with each other. Defining the roles and responsibilities of such groups can help to strengthen the governance of LISCC cybersecurity supervision.

S&R Has Undergone Several Structural Changes Affecting Its Governance of LISCC Firm Cybersecurity Supervision

S&R has undergone several structural changes over the past several years, affecting its governance approach to LISCC firm cybersecurity supervision. According to the Institute of Internal Auditors Research Foundation, effective organizational governance includes systems and associated processes and structures for an organization's decisionmaking, accountability, controls, and behaviors that help an organization accomplish its objectives.[10]

In 2015, S&R launched the CPG within the division's policy function to improve and further develop the System's oversight of cybersecurity for all portfolios. This initiative sought (1) to issue cybersecurity risk policy and set expectations for financial institutions, (2) to develop examiner supervisory programs, (3) to build a cybersecurity surveillance and risk analysis infrastructure, (4) to increase cybersecurity training and assign examiners to institutions with the most risk, and (5) to implement robust continuous monitoring of cybersecurity risk-management program effectiveness at financial institutions. Board and Reserve Bank interviewees noted that although the CPG had some successes, such as recruiting cybersecurity specialists across the System and providing a mechanism for coordinating and responding

[10] Dean Bahrman, *Evaluation and Improving Organizational Governance,* The Institute of Internal Auditors Research Foundation, 2011.

quickly to cybersecurity incidents, it lacked sufficient authority to implement its overall plans for the supervisory portfolios.

In 2018, the Board reorganized the LISCC program. The new structure consolidated the supervision of nonfinancial risks, including cybersecurity, under the G&C core assessment program. In 2019, S&R reorganized the division into three functions—supervision, policy, and operations—to better align the division's structure with its primary activities and its mission and strategy. As part of that reorganization, S&R established the BTR section within the supervision function. The BTR section seeks to develop and coordinate an integrated supervisory program across all portfolios for IT and IT-related areas, including cybersecurity.[11] Board officials noted that although the BTR section seeks to influence the allocation of resources to the supervisory portfolios with the greatest risk, the LISCC program retains authority for LISCC firm supervisory planning and execution through its G&C program. The BTR section is in the nascent stages of its development, and one of its early objectives is to establish a governance structure.

In January 2020, S&R dissolved the CPG, stating that many of its responsibilities had shifted to the BTR section in the division's supervision function and S&R's Systems and Operational Resiliency Policy (SORP) section in the division's policy function. SORP seeks to enhance S&R's strategic policy framework for supervised institutions concerning operational resiliency, cybersecurity, IT, and emerging technology.

In May 2020, the BTR section established a charter for an oversight group. According to the charter, the oversight group will facilitate communication, coordination, collaboration, and efficient sharing of resources; participate in or provide resources for subgroups and projects initiated by the oversight group; and coordinate communication with the Board on relevant areas of discussion. As of August 2020, the BTR section was in the process of finalizing the membership of its oversight group and was planning to hold the oversight group's initial meeting later that month.

The plan to develop an integrated approach to IT supervision, including cybersecurity supervision, through the creation of the BTR section should help S&R take a more holistic approach to assessing how firms use technology and the risks associated with technology. Our interviews with program officials revealed that the reorganization of the LISCC program, along with the formation of the BTR section and the subsequent dissolution of the CPG, has created a need to clarify the roles and responsibilities pertaining to LISCC firm cybersecurity supervision and planning.

Structural Changes Have Created a Need to Clarify Roles and Responsibilities Pertaining to LISCC Firm Cybersecurity Supervision and Planning

Board and Reserve Bank interviewees described challenges that they encountered while operating under the evolving governance structure. Several interviewees stated that the roles, responsibilities, reporting relationships, authorities, and objectives for LISCC cybersecurity supervision were unclear. For example, Board and Reserve Bank officials indicated that no formal plan had been implemented to guide the

[11] S&R established the BTR section following the results of a 2017 internal assessment that proposed modernizing S&R's IT supervision. That assessment called for expanding coverage of IT and taking a holistic approach to assessing firms' business technology risks.

transition following the dissolution of the CPG. In addition, an interviewee indicated that the coordination and connection among SORP, the BTR section, and the supervisory portfolios are not clear and that defining a governance structure would help. Based on our interviews and analysis, we identified additional areas for potential clarification, including the reporting line and objective for the cybersecurity horizontal team, the approach to coordinating interagency cybersecurity examinations, and the role of certain cross-portfolio groups in cybersecurity supervision planning.[12]

Reporting Line and Objective for the Cybersecurity Horizontal Team

Board and Reserve Bank interviewees noted that the reporting line and objective for the LISCC cybersecurity horizontal team were unclear. For example, a Reserve Bank interviewee explained that it is not clear how the cybersecurity team fits into the overall structure of the LISCC program. We noted that the LISCC program recently updated its organizational chart to clarify the reporting line for its cybersecurity horizontal team; however, the G&C operating manual has not been updated to reflect the addition of the cybersecurity team to the LISCC program or to provide detail on the team's mission or objective. A Board official noted that although the Board has goals and objectives for the G&C program, this official was not aware of any objectives for cybersecurity supervision. In addition, a Reserve Bank interviewee noted that the LISCC program has not clearly defined the mission of the cybersecurity team.

Approach to Coordinating Interagency Cybersecurity Examinations

We learned that S&R is in the planning stages of an interagency cybersecurity examination that will involve some LISCC firms. Although the LISCC program is responsible for approving proposed examination activities at LISCC firms, including cybersecurity horizontal and idiosyncratic examinations, one of the BTR section's objectives is to ensure that its program aligns with and complements interagency work. Accordingly, the BTR section is involved in planning this interagency horizontal examination. However, it is unclear how the LISCC program and the BTR section will coordinate their planning efforts and how this or future interagency reviews will inform or affect other supervisory plans for LISCC firms. According to a Board official, the BTR section plans to ensure that interagency coordinated examination work is not duplicative of the cybersecurity work conducted by the LISCC program and other federal financial regulators.

Role of Certain Cross-Portfolio Groups in Cybersecurity Supervision Planning

The way in which cybersecurity information from certain cross-portfolio groups contributes to the selection of topics and focus areas for LISCC cybersecurity horizontal examinations and idiosyncratic work is not clearly defined. The *LISCC Program Manual* describes the planning process for LISCC firms as follows:

[12] *Cross-portfolio groups* are System groups that identify risks to support S&R's various supervisory portfolios, such as the LISCC portfolio, the large and foreign banking organization portfolio, and the regional banking organization portfolio, among others.

- LISCC supervision planning inputs include the proposals and risks identified by the MAP, the G&C steering committee, and the G&C program leadership group, as well as the DSTs. The LISCC program's annual prioritization and planning process begins with an annual outlook briefing, which has two main components: (1) a summary of outstanding and emerging idiosyncratic and horizontal supervisory issues from each core assessment program, including the G&C program, and (2) a briefing on the current risks and trends across the portfolio from the MAP.
- Each LISCC core assessment program proposes supervisory work for the LISCC Operating Committee's consideration. For the G&C program, this includes horizontal examinations, idiosyncratic examinations, and supervisory issue follow-up. The DSTs then provide the LISCC Operating Committee with the full set of supervisory work proposed for its respective firms. The program leadership groups for each of the core assessment programs work with the DSTs and the horizontal teams in their respective program to develop a proposed body of idiosyncratic and horizontal work to be conducted over the next supervisory cycle.

In addition to the MAP and the DSTs within the LISCC program, other groups play a role in identifying and tracking cybersecurity risks across the supervisory portfolios, including the LISCC portfolio:

- The Cybersecurity Analytics Support Team (CAST) performs cybersecurity threat analyses, assesses the severity of cybersecurity incidents, recommends supervisory actions, and provides situational awareness updates. CAST monitors cybersecurity developments and events across the financial sector and critical payment, clearing, and settlement systems. Additionally, CAST's role is to raise awareness around cybersecurity threats to influence the supervisory process.
- The Cybersecurity Risk Analysis Team focuses on assessing the effect of cybersecurity risks on the financial sector. This team produces an assessment of current and potential cybersecurity risks. A Reserve Bank official noted that the assessment includes a list of horizontal cybersecurity examination themes that it views as having the greatest potential to reduce risk across the financial sector and future possible risk trends. One interviewee noted that CAST also supports the Cybersecurity Risk Analysis Team's efforts.

The role of these groups in the supervisory planning process, however, is not formally defined. Interviewees indicated that there is an opportunity to improve the cybersecurity planning process by defining or formalizing the approach to incorporating input from CAST and the Cybersecurity Risk Analysis Team. A Board official noted that since the dissolution of the CPG, there is no formal process for SORP to ensure that information from CAST and the Cybersecurity Risk Analysis Team is incorporated into the supervision planning process. Another Board official noted that one of the goals of the BTR section is to ensure that the Cybersecurity Risk Analysis Team's work contributes to the supervisory planning process and coincides with the timing of supervisory planning. The same official noted that although this team had been providing reports on cybersecurity themes, it was not clear how the reported information contributed to the supervisory planning process. Given the rapidly evolving pace of cybersecurity threats, defining the approach to gathering insights from CAST and the Cybersecurity Risk Analysis Team could help the LISCC program to incorporate additional information on cybersecurity threats and issues to support supervisory planning.

Conclusion

Given the considerable structural changes recently implemented and under development related to cybersecurity and the supervision of LISCC firms, as well as the dynamic nature of cybersecurity risks, we believe that it is important to define the roles and responsibilities pertaining to LISCC cybersecurity supervision and planning. Defining these roles and responsibilities can help strengthen the governance of LISCC cybersecurity supervision.

Recommendations

We recommend that the director of S&R

1. Formalize the governance of LISCC cybersecurity supervision to clarify roles, responsibilities, and authorities of the LISCC program and other groups that may play a role in LISCC cybersecurity supervision matters, such as the BTR section.
2. Update the G&C operating manual to reflect the position of the cybersecurity horizontal team within the LISCC program and establish a clear objective for that team.
3. Develop a plan to ensure that the LISCC program, in consultation with the BTR section, incorporates interagency coordinated reviews in its supervisory planning processes for LISCC firms.
4. Develop a plan to define how cybersecurity information from cross-portfolio groups, such as CAST and the BTR section, contributes to the planning process for LISCC cybersecurity supervision activities.

Management Response

In its response to our draft report, the Board concurs with our recommendations. The Board states that S&R has undergone several structural changes affecting its governance of cybersecurity supervision within the LISCC program and supervision more broadly. The Board also notes that responsibility for governance lies within the LISCC program, the BTR section, and S&R's policy function. The Board also recognizes the need for its policies, processes, and partnerships to align with and clarify current practices.

Specifically, in response to recommendation 1, the Board states that by the end of 2020, it will ensure that its governing manuals and charters reflect the current roles, responsibilities, and authorities of the groups involved in LISCC cybersecurity matters. The Board further notes that it has already established overlapping membership on governing bodies, such as the G&C steering committee and the BTR oversight group.

In response to recommendation 2, the Board states that by the end of 2020, it will update its governing manuals and organization charts, as appropriate, to include the cybersecurity horizontal team and its objective.

In response to recommendation 3, the Board states that the interagency coordinated reviews are included in the 2020 and 2021 supervisory plans and have priority for LISCC cybersecurity examination

resources. The Board further notes that the LISCC G&C program is involved in the development of the interagency reviews.

In response to recommendation 4, the Board states that during the supervisory planning process, it considers a wide range of intelligence from inside and outside the System, including information from CAST, and that the BTR section participates in the process. The Board further notes that by the end of 2020, it will formalize its processes for soliciting input from cross-portfolio groups.

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 LISCC Program Can Better Define How to Factor the Results of Cybersecurity Supervision Activities Into Firm G&C Ratings

The Board can better define how cybersecurity supervisory activities inform the G&C ratings of LISCC firms. The Board recently updated its rating framework for large financial institutions and has not yet issued guidance on the relative importance of the cybersecurity assessment to a firm's G&C rating. Clarifying how weaknesses or deficiencies identified during cybersecurity supervision activities factor into G&C ratings can help the LISCC program better communicate its assessment regarding firms' cybersecurity posture.

The LISCC Program Has Not Defined Expectations for How Its Cybersecurity Supervisory Activities Inform the G&C Rating of the Newly Established LFI Rating System

The G&C program is responsible for evaluating LISCC firms' IT, information security, and cybersecurity governance processes, among other areas; however, officials indicated that it is unclear how to incorporate the results of these cybersecurity supervision activities into the annual G&C rating. We attribute this lack of clarity to the LISCC program not having clearly defined expectations for how to incorporate the results of cybersecurity supervision activities when determining this rating within the new LFI rating system.

We determined that the G&C program's operating manual does not indicate the relative importance of cybersecurity assessments in the G&C rating. The *Large Financial Institution Rating System*,[13] which took effect in February 2019, does not specify the role of cybersecurity, IT, or information security supervisory work in determining the G&C rating. Under this rating system, the G&C rating assesses a firm's effectiveness in aligning strategic business objectives with its risk appetite and risk management capabilities, maintaining effective and independent risk management and control functions, promoting compliance with laws and regulations, and otherwise providing for the ongoing resiliency of the firm. The Board does not have guidance on how supervisory staff should consider cybersecurity risk in the LFI rating system.

Officials said it was unclear how to incorporate cybersecurity examination work into the G&C rating. Some officials noted that they would be reluctant to assign a G&C rating based on the cybersecurity

[13] Board of Governors of the Federal Reserve System, *Large Financial Institution (LFI) Rating System*, SR 19-3/CA 19-2, February 26, 2019. See also 83 Fed. Reg. 58724 (Nov. 21, 2018) and 84 Fed. Reg. 4309 (Feb. 15, 2019) for more information.

supervisory work performed, noting that the LISCC program has not yet conducted sufficient cybersecurity examination work to form an assessment to support a G&C rating. One official said cybersecurity issues would need to be combined with weaknesses in other areas to justify a G&C rating determination. By clarifying how concerns identified during cybersecurity supervisory activities factor into the G&C rating, the LISCC program can better communicate its supervisory expectations and its preferred approach for this ratings determination.

Recommendation

We recommend that the director of S&R

5. Define the steps for considering the results of cybersecurity supervisory activities when determining LISCC firms' G&C rating within the new LFI rating system.

Management Response

In its response to our draft report, the Board concurs with our recommendation. The Board states that by the end of 2020, it plans to establish a formal process for aggregating and considering the results of cybersecurity supervisory activities in determining the G&C rating and for ensuring that the results are escalated for consideration by the G&C steering committee and other governing bodies, as appropriate. The Board notes that it will use these steps in the G&C ratings process currently planned for the first quarter of 2021.

OIG Comment

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

Finding 3: The LISCC Program Can Enhance Its Approach to Cybersecurity Training

Some cybersecurity examiners have difficulty obtaining training, and several interviewees noted that minimum skills and training expectations for cybersecurity examiners are unclear. According to the National Institute of Standards and Technology's *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, a critical aspect of a skilled cybersecurity workforce involves developing and retaining skilled talent. Interviewees cited multiple reasons for these training issues, including an unstructured and decentralized approach to training LISCC cybersecurity specialists as well as time constraints imposed by other job duties. Some interviewees expressed concern that cybersecurity examiners' skills may become outdated without sufficient and timely training on emerging cybersecurity and IT topics. The inability of cybersecurity examiners to keep their skills updated could affect their readiness to examine emerging cybersecurity risk areas and may also affect the LISCC program's retention rates. Additionally, the lack of a structured and centralized training program hinders the LISCC program's ability to hire less experienced cybersecurity examiners and develop their skills over time.

Some Cybersecurity Examiners Have Difficulty Obtaining Training

Many interviewees described an unstructured and decentralized approach to training LISCC cybersecurity specialists. Several other interviewees stated that some cybersecurity examiners have difficulty obtaining training, and one interviewee explained that cybersecurity examiners' training needs were not being met because of the LISCC program's approach to cybersecurity training. In addition, interviewees indicated a lack of clarity around minimum skills and training expectations for cybersecurity examiners. A Reserve Bank official stated that the G&C program relies on individual development plans instead of a structured cybersecurity training plan. The training section of the G&C program's operating manual was incomplete as of April 2020.

Multiple cybersecurity examiners noted that there is no framework or structure to identify and develop the most important cybersecurity skill sets. As indicated in the *NICE Cybersecurity Workforce Framework*, a critical aspect of a skilled cybersecurity workforce involves developing and retaining skilled talent. In 2017, the CPG developed a National Cyber Risk Specialist Program to create and train a Systemwide pool of cybersecurity experts; however, S&R terminated this program following the dissolution of the CPG. A Board official explained that the BTR section's workforce planning initiative may include a training program for cybersecurity specialists and IT examiners, but the BTR program would first need to identify skill sets and determine how to develop them. Currently, instead of centralized training within the LISCC program, each Reserve Bank independently determines its approach for identifying and providing cybersecurity examiner training opportunities.

In addition, each Reserve Bank involved in supervising LISCC firms establishes its own training budget, regardless of whether it has IT and cybersecurity examiners assigned to the LISCC program. Our analysis found that Reserve Bank training budgets for cybersecurity examiners in 2019 varied considerably—in

some instances by thousands of dollars. One Reserve Bank spent over three times more per cybersecurity examiner than any of the other three Reserve Banks that have at least one LISCC firm in the Reserve Banks' District.[14] Interviewees at some Reserve Banks told us that training budget limitations make it difficult for examiners to receive adequate cybersecurity training to keep their cybersecurity knowledge current. Several cybersecurity examiners stated that they have had training requests denied or have not requested to attend a training because of budget constraints.

A Board official noted that it is difficult to keep cybersecurity examiners' knowledge current given the high cost of relevant training and that in the past, the Board has had to come up with creative solutions to address this issue. For example, a Reserve Bank official explained that it was necessary to move budget resources from other teams to meet the needs of cybersecurity examiners because they would not be able to do their jobs without the training.

Some cybersecurity examiners also have had difficulty attending training because of time constraints imposed by supervisory activities, including examinations, follow-up on Matters Requiring Attention and Matters Requiring Immediate Attention, and monitoring activities. Reserve Bank officials acknowledged that cybersecurity examiners' workload often constrains their availability to attend training. A Reserve Bank official explained that the CAST function has begun distributing informational products on current and emerging threats to cybersecurity examiners, in part to mitigate the challenge of maintaining and updating cybersecurity examiner skill sets.

Training Difficulties Impede Cybersecurity Examiner Development, Retention, and Hiring Efforts

Interviewees expressed some concern that cybersecurity examiners' skills may become outdated if they do not receive sufficient and timely training on emerging cybersecurity and IT topics. We believe that when cybersecurity examiners' skills become outdated, they may be less aware of emerging threats and the latest approaches to mitigating those threats, which may hinder the effectiveness of their supervisory activities.

Further, the inability of cybersecurity examiners to keep their skills updated could adversely affect retention rates. Cybersecurity examiners have established relationships, institutional knowledge, and organizational experience that are difficult to replace in the event of turnover. Therefore, examiner turnover may lead to increased recruitment costs and training expenses, diminished productivity, and reduced morale.

Additionally, we believe the lack of a structured and centralized training program hinders the LISCC program's ability to hire less experienced cybersecurity examiners and train them to enhance and develop their skills to become more effective in the role. One Reserve Bank official responsible for hiring cybersecurity examiners explained that hiring experienced cybersecurity talent is expensive and difficult. The official noted that peer federal financial regulators have better cybersecurity examiner training

[14] As of June 2020, the 11 firms in the LISCC portfolio are located in the Districts of the Federal Reserve Banks of Boston, New York, Richmond, and San Francisco.

programs and that the LISCC's current training program is not effective enough to allow the program to hire less experienced candidates. Another interviewee with prior experience managing a formal training program for IT and cybersecurity examiners at a peer federal financial regulator stated that adopting a formal training program would be beneficial.

Recommendations

We recommend that the director of S&R

6. Develop a structured cybersecurity training plan for cybersecurity examiners. As part of the plan, define expectations for skill sets and for continuing education, such as training related to emerging risks.
7. Require that relevant examiners complete cybersecurity training in a manner consistent with the plan to address recommendation 6.

Management Response

In its response to our draft report, the Board concurs with our recommendations. The Board acknowledges that its current approach to cybersecurity training is unstructured and decentralized and states that enhancements to cybersecurity examiner training will extend beyond the LISCC program. The Board states that S&R's cross-portfolio operational resilience group has an objective to address workforce development and training across IT skills, including cybersecurity. The Board states that the operational resilience group will establish a program framework for cybersecurity examiner training across the System and will work with other groups as appropriate to implement and deliver the training. The Board also states that the operational resilience group will work with supervisory portfolios to establish skill set and continuing education expectations, as well as training requirements. The Board intends to implement these recommendations by the end of 2021.

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 4: The Board Can Enhance Guidance and Training on Reporting Cybersecurity Events

As of February 2020, only a limited number of cybersecurity incidents had been reported in the Cyber Event Repository (CER) for LISCC firms, and some Reserve Bank examiners reported that they are unclear on how to use the system. The *S&R Policy Development and Implementation Guide* states that the policy function of S&R aims to develop clear and concise policies that are useful and timely for System examiners and for the banking industry and to promote consistent and effective implementation of policies across the System, among other things. Board guidance for the CER, which was established to record information about cybersecurity incidents and incidents reportable under the Gramm-Leach-Bliley Act (GLBA) and the act's interagency interpretive guidance, does not clearly state the types of cybersecurity incidents that should be recorded in the system and is fragmented across three different guidance documents. Further, CER users have limited access to training and guidance. Absent clear, centralized guidance and training, CER users may not be consistently entering cybersecurity events into the CER, increasing the likelihood that the System may not be effectively and timely synthesizing information on cybersecurity incidents.

Guidance for the CER Is Fragmented and Unclear

In April 2018, the Board established the CER to record and track information about security incidents.[15] CAST has oversight responsibility for the CER and also performs cybersecurity threat analyses; assesses the severity of cybersecurity incidents; recommends supervisory actions to central points of contact (CPCs), DSTs, and other internal stakeholders; and provides situational awareness updates.[16]

Three separate guidance documents issued by the Board address the use of the CER:

- April 2018 guidance implementing the CER
- December 2018 guidance that details roles, responsibilities, and processes for responding to cybersecurity incidents
- a playbook that seeks to establish procedures and protocols for effective, consistent, and replicable supervisory actions in response to cybersecurity incidents

In its April 2018 guidance implementing the CER, the Board directed CPCs, or their designees, to open a new record in the CER for each unique incident notification provided by a financial institution pursuant to Supervision and Regulation Letter 05-23, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (response guidance). The response guidance

[15] The CER includes information from firms in all supervisory portfolios. We focused our analysis on CER data associated with LISCC firms, and we interviewed CER users assigned to supervise LISCC firms.

[16] A DST lead serves as the team lead for LISCC firm supervision. For the purposes of this report, *CPC* is equivalent to *DST lead*.

interprets GLBA and the *Interagency Guidelines Establishing Information Security Standards* (security guidelines) and directs financial institutions supervised by the Board to promptly contact their Reserve Bank's CPC to report security incidents involving sensitive customer information.[17] The response guidance also requires financial institutions to report security incidents involving sensitive customer information to their primary federal regulator.[18] In addition, the Board's April 2018 guidance encourages Reserve Bank CPCs, or their designees, to enter into the CER those security incident notifications that do not involve sensitive customer information, including security incidents that a financial institution voluntarily reports or that examiners identify in the normal course of supervision.

In December 2018, the Board issued guidance on the roles, responsibilities, and processes for responding to cybersecurity incidents as well as other events involving significant operational impact. This guidance details the responsibilities of key stakeholders, including CPCs, CAST, and SORP. For example, the guidance states that CAST and SORP will jointly perform after-action reviews following significant cybersecurity events to identify procedural improvements that SORP will then incorporate into the playbook described below. This guidance states that it applies to cybersecurity incidents reported in accordance with the response guidance and those reported voluntarily during an examination or through the normal course of supervision and entered into the CER by Reserve Bank staff. Neither the April 2018 guidance nor the December 2018 guidance defines *cybersecurity incidents* for the purposes of reporting in the CER.

The December 2018 guidance references a playbook that seeks to establish procedures and protocols for supervisory actions in response to cybersecurity incidents with the potential to affect financial institutions supervised by the System. This playbook defines cybersecurity incidents in a footnote as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an institution's information systems or the information residing therein."

However, the guidance in the playbook addressing the CER is similar to the Board's April 2018 guidance—it states that CPCs should enter in the CER all cybersecurity incidents reported to them by supervised institutions that involve unauthorized access to or use of sensitive customer information. Also like the April 2018 guidance, it does not specify which other types of cybersecurity incidents, if any, should be entered into the CER. Additionally, we noted that the playbook references the CPG executive oversight

[17] The response guidance interprets the requirements of section 501(b) of GLBA, 15 U.S.C. § 6801, and the security guidelines to include the development and implementation of a response program to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. Section 501(b) requires the appropriate federal banking agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards (1) to ensure the safety and confidentiality of customer information, (2) to protect against any anticipated threats or hazards to the security or integrity of such information, and (3) to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any 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.

[18] For the purposes of the response guidance, 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 Board is not the primary federal regulator for all the subsidiaries of the domestic bank holding companies and foreign banking organizations in the LISCC portfolio.

group, which S&R dissolved. In December 2019, a CAST employee told us that CAST would update the playbook to remove these outdated references. As of May 2020, the playbook had not been updated.

Thus, the guidance on what types of incidents should be recorded in the CER is fragmented across three guidance documents and does not clearly define what types of cybersecurity incidents should be recorded in the system. The *S&R Policy Development and Implementation Guide* states that the policy function of S&R aims to develop clear and concise policies that are useful and timely for System examiners and for the banking industry and to promote consistent and effective implementation of policies across the System, among other things. Without clear, centralized, and up-to-date guidance, CER users may not be consistently entering cybersecurity events into the CER, increasing the likelihood that the System may not be effectively and timely synthesizing information on cybersecurity incidents.

Some Reserve Bank Examiners Are Unclear on How to Use the CER

Some Reserve Bank examiners we spoke with expressed confusion about which types of cybersecurity events they should enter into the CER. In addition, some examiners told us that they did not understand how to complete some fields in the CER system or the level of detail to include in certain fields. Further, several examiners raised concerns regarding the workload associated with entering information into the CER and stated that recording every cybersecurity event—regardless of severity—in the system would take a significant amount of time. According to a CAST employee, the amount of time it takes a CPC, or their designee, to collect and analyze this information can vary significantly, ranging from a few minutes to several hours. The employee added that many supervisory teams prefer to attach internal memorandums that they have already written, and that in these instances, CAST employees review the memorandums and populate the fields in the CER. The employee also noted that CAST employees often assist CPCs, or their designees, with completing some of the more technical fields in the CER.

According to the playbook, after a user opens an incident in the CER, they should collect additional information**.** As new information is collected and analyzed, the user should continue to monitor the institution's response to the incident and assess risks and responses from a safety and soundness perspective, as well as ensure that appropriate consumer protections are in place. However, we found that as of February 2020, 9 of the 24 incidents that were open in the CER had not been updated in more than a year.

According to a CAST employee, once the user has entered the required information into the CER, a member of CAST reviews the information and determines whether to close the incident. The employee stated that, because of CAST staff resource constraints, there is a backlog of incidents in the CER for CAST to review and, if appropriate, close. As of February 2020, CAST has closed just 2 of the 26 cybersecurity incidents pertaining to LISCC firms in the CER.

According to a CAST employee, there are several factors that CAST considers when determining whether to close an incident. For example, CAST may decide to close an incident if it was unable to obtain any additional information regarding the issue, or it may decide to close an incident if a financial institution has addressed the issue. The CAST employee added that although CAST is responsible for closing incidents in the CER, the decision to close an incident is made in consultation with the CPC. A BTR employee stated that the BTR section plans to coordinate how CAST will provide inputs into the

supervision process. This employee also noted that cybersecurity incident reporting did not always occur as CAST intended but added that the BTR section will be promoting this reporting as part of its responsibilities.

CER Users Have Limited Access to Training and Guidance

CAST has provided limited guidance and training on how to use the CER. CAST has developed a user manual to provide information to CPCs and their designees on how to enter information into the CER; however, a CAST employee stated that the user manual has been in draft form for 2 years because of staff resource constraints and was never shared with users. In May 2020, a CAST employee estimated that the user manual would be finalized in July 2020.

A CAST employee stated that CAST provided one training session on the CER, but that the training session focused on awareness of the CER rather than a discussion of expectations for using the system and that attendance was not required. According to this employee, CAST does not maintain records of training and places a certain amount of reliance on the Reserve Banks to ensure that users know how to use the CER. Further, this employee stated that identifying who should take the training can be difficult because CAST does not know which Reserve Bank examiners are responsible for each of the firms in the LISCC portfolio.

A CAST employee stated that CAST was planning to hold a training session after the playbook is updated, and that the training would be mandatory for a large portion of supervision management and employees. The employee added that this training would reinforce the Board's April 2018 and December 2018 guidance on the CER and provide an overview of the playbook.

The CER Contains Few LISCC Firm Incidents and Missing Information

As of February 2020, few LISCC firm incidents had been recorded in the CER. From April 2018 through February 2020, we found that there were only 26 incidents for six LISCC firms recorded in the CER. Representatives from the LISCC firms we interviewed stated that they share information on cybersecurity incidents during their quarterly meetings with the DSTs. However, one of these representatives expressed concern that firms are not reporting cybersecurity incidents consistently and stated that it would be beneficial to have guidance that clarifies what types of cybersecurity incidents financial institutions should report to the System. A CAST employee stated that based on the number of entries in the CER, there is reason to believe that there is underreporting of both incidents involving sensitive customer information and cybersecurity incidents.[19]

[19] The Board is not the primary federal regulator for all the subsidiaries of the domestic bank holding companies and foreign banking organizations in the LISCC portfolio. We acknowledge that these subsidiaries, such as national banks, may be reporting incidents to their primary federal regulator. During our evaluation, we did not evaluate firms' reporting to their primary federal regulators.

Further, many of the entries in the CER are missing key information that CAST uses to determine whether an event involves sensitive customer information, which financial institutions are required to report under the response guidance and the security guidelines, or whether an event is a cybersecurity incident, which financial institutions may voluntarily report.[20] For example, only 3 of the 26 entries include information on whether the incident included sensitive customer information. In addition, only 11 of the 26 entries include information on whether the incident was intentional or accidental, which is one of the fields that CAST uses to determine whether an event is a cybersecurity incident. Given the limited information reported in the CER, the LISCC program and CAST may not know the entirety of cybersecurity incidents at LISCC firms.

Recommendations

We recommend that the director of S&R

8. Update the Board's April 2018 guidance on the CER to clearly define the types of cybersecurity events that should be entered into the system.
9. Develop instructions and training on using the CER, and issue guidance that requires CPCs, or their designees, to complete this training.
10. Update the cybersecurity incident playbook to reflect S&R's current organizational structure.

Management Response

In its response to our draft report, the Board concurs with our recommendations. The Board states that enhancements to cybersecurity event reporting include and extend beyond the LISCC program and that CAST has been working to enhance this reporting. Specifically, in response to recommendation 8, the Board states that it plans to update the CER guidance to clearly define the types of events that should be entered into the system. In response to recommendation 9, the Board states that it plans to develop instructions and training on using the CER and require CPCs or their designees to complete the training. In response to recommendation 10, the Board states that it plans to update the cybersecurity incident playbook to reflect changes in S&R's organizational structure. The Board notes that it plans to implement recommendations 8 and 9 by the end of 2021 and recommendation 10 by the end of June 2021.

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.

[20] Although firms are required to report incidents involving sensitive customer information under the response guidance and the security guidelines, the reporting of cybersecurity incidents that do not involve sensitive customer information is not required by law or suggested by guidance to firms. Although internal guidance suggests that examiners should report cybersecurity incidents that do not involve sensitive customer information in the CER, the availability of that information to CAST and the LISCC program depends on voluntary reporting by firms or information that examiners may discover during the normal course of supervision.

Appendix A: Scope and Methodology

The scope of our evaluation included applicable laws, regulations, policies, procedures, and agency practices related to the cybersecurity supervision of LISCC firms. We reviewed the cybersecurity supervision activities executed by the LISCC program and the four Reserve Banks with LISCC firms in their Districts—the Federal Reserve Banks of Boston, New York, Richmond, and San Francisco. Our scope did not include firms in the community banking organization, regional banking organization, or large and foreign banking organization portfolios, nor did our scope include supervisory activities unrelated to cybersecurity.

To accomplish our objective, we reviewed relevant statutes and regulations, Board guidance, high-priority initiatives, strategic roadmaps, meeting minutes, and program manuals applicable to cybersecurity supervision and the LISCC program. We also reviewed interagency guidance related to cybersecurity supervision. We analyzed the topics, time frames, and LISCC firm coverage for cybersecurity horizontal examinations performed or planned from 2015 to 2020. We reviewed supervisory information and documents for idiosyncratic cybersecurity supervisory activities that are completed, planned, or in progress from 2016 to 2020 at each of the LISCC firms, including cybersecurity examination reports and scope memorandums, memorandums related to Matters Requiring Attention and Matters Requiring Immediate Attention follow-up activities, and documents related to monitoring activities. We also reviewed LISCC MAP documents related to cybersecurity monitoring activities.

We obtained and analyzed information from the Federal Reserve Banks of Boston, New York, Richmond, and San Francisco on their 2019 training budgets and expenses for cybersecurity examiners assigned to the LISCC program. We also obtained and analyzed incident information reported in the CER for LISCC firms from April 1, 2018, through February 29, 2020.

We conducted more than 50 interviews of Board and Reserve Bank officials and employees to gain their perspectives on the LISCC program's cybersecurity activities. We interviewed Board and Reserve Bank officials who oversee the LISCC program; Board officials responsible for S&R's SORP section and BTR section; Reserve Bank officials and employees responsible for CAST; an official with the Federal Reserve Bank of New York cybersecurity policy group; and officials and examiners from the Federal Reserve Banks of Boston, New York, Richmond, and San Francisco who are responsible for cybersecurity supervision of LISCC firms, including officials and examiners assigned to the LISCC G&C program and individual LISCC firm DSTs.

We also requested interviews with representatives from six selected LISCC firms to obtain their perspectives on the LISCC program's cybersecurity supervision approach and activities. When we selected the LISCC firms to interview in December 2019, there were 12 firms in the Board's LISCC program. In selecting from those 12 firms, we considered the scale of the firm's operations, the firm's most recent LFI G&C ratings, and the firm's responsible Reserve Bank. As of June 2020, we had interviewed representatives from three of the six LISCC firms we selected; we were unable to schedule interviews with the remaining three firms. Although we aimed to interview representatives from a cross-section of LISCC firms to capture a broad understanding of their views on cybersecurity supervision, we cannot generalize the results from our selection across the population of LISCC firms.

We conducted our fieldwork from April 2019 through June 2020. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation*, issued in January 2012 by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B: Management Response

Large Institution Supervision Coordinating Committee (LISCC)
Management Response to the OIG Cybersecurity Review

FRS LISCC

Michael VanHuysen
Associate Inspector General
For Audit and Evaluations
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Dear Mr. VanHuysen,

Thank you for the opportunity to comment on your draft report, *The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced.* We appreciate the effort that the Office of the Inspector General (OIG) put into this report, the recognition that our approach continues to evolve in this area, and the recommendations provided for enhancing the effectiveness of the Board's approach to cybersecurity supervision.

The report addresses four areas of cybersecurity supervision and event monitoring for enhancement: governance of LISCC firm cybersecurity supervision, process for considering cybersecurity findings within the ratings of the LISCC firms, cybersecurity training for examiners, and guidance and training for cybersecurity event reporting. The Division of Supervision and Regulation agrees with the conclusions and recommendations in the report for these areas.

Governance of LISCC Firm Cybersecurity Supervision Can Be Strengthened

The report recognizes that S&R has undergone several structural changes affecting its governance of cybersecurity supervision within LISCC and supervision more broadly, as governance elements lie within LISCC, the Board's Business Technology Risk group, the Board's Policy Group and the recent interagency coordinated examination effort. There's a need for our formal policies, processes, and partnerships to align with and clarify current practices.

> *Recommendation 1: Formalize the governance of LISCC cybersecurity supervision to clarify roles, responsibilities, and authorities of the LISCC Program and other groups that may play a role in LISCC cybersecurity supervision matters, such as the BTR section.*
>
> By the end of 2020, we will ensure our governing manuals and charters reflect the current roles, responsibilities, and authorities of the groups involved in LISCC cybersecurity matters. We have already established cross-membership on governing bodies, such as the G&C Steering Committee and BTR Oversight Group.
>
> *Recommendation 2: Update the G&C operating manual to reflect the position of the cybersecurity horizontal team within the LISCC program and establish a clear objective for that team.*
>
> By the end of 2020, we will update our governing manuals and organizational charts, as appropriate, to reflect the inclusion and objective of the cybersecurity horizontal team.

Page 1 of 4
Published: 09/22/2020

Recommendation 3: Develop a plan to ensure that the LISCC program, in consultation with the BTR section, incorporates interagency coordinated reviews in its supervisory planning processes for LISCC firms.

The interagency coordinated reviews are included in the 2020 and 2021 supervisory plans and have priority for LISCC cybersecurity examination resources. LISCC G&C has representation within the project teams for the development of the interagency program and within leadership groups.

Recommendation 4: Develop a plan to define how cybersecurity information from cross-portfolio groups, such as CAST and the BTR section, contributes to the planning process for LISCC cybersecurity supervision activities.

The supervisory planning process already considers a wide range of intelligence from inside and outside the Federal Reserve System, receiving information from CAST and participating with BTR. By the end of 2020, we will formalize our processes for soliciting input from cross-portfolio groups.

The LISCC Program Can Better Define How to Factor the Results of Cybersecurity Supervision into Firm G&C Ratings

The report recognizes that cybersecurity supervisory activities are one of several elements that factor into the G&C rating within the LFI Rating System that became effective in February 2019. The report appropriately identifies that cybersecurity risk management and controls are embedded within the ratings without specifying the role of the work in determining the G&C rating. Other risks and considerations are treated similarly to cybersecurity for the purposes of the rating process.

Recommendation 5: Define the steps for considering the results of cybersecurity supervisory activities when determining LISCC firms' G&C rating within the new LFI rating system.

By the end of 2020, we will establish a formal process for aggregating and considering the results of cybersecurity supervisory activities in the determination of the G&C rating, ensuring the results are escalated for consideration by the G&C Steering Committee and other governing bodies, as appropriate. These steps will be utilized in the ratings process currently planned for the first quarter of 2021.

The LISCC Program Can Enhance its Approach to Cybersecurity Training

We agree with the report's indication that our current cybersecurity training program is unstructured and decentralized. We recognize and share many of the concerns expressed in the report, and that the enhancements extend beyond the LISCC portfolio examiners. The cross-portfolio Operational Resilience group has an objective for workforce development and training across IT skills, which includes cybersecurity.

Recommendation 6: Develop a structured cybersecurity training plan for cybersecurity examiners. As part of the plan, define expectations for skill sets and continuing education, such as training related to emerging risks.

Recommendation 7: Require that relevant examiners complete cybersecurity training in a manner consistent with the plan to address recommendation 6.

By the end of 2021, the Board's Operational Resilience group will establish a program framework for cybersecurity examiner training for the Federal Reserve System, working with other groups as appropriate for the implementation and delivery of the training. In concert with that training program, the Operational Resilience group will work with supervisory portfolios to establish skill set and continuing education expectations, and required training.

The Board Can Enhance Guidance and Training on Reporting Cybersecurity Events

The report highlights the enhancements needed to improve the consistency of our cybersecurity event reporting. These enhancements are System-wide, including and extending beyond LISCC supervision. We agree with the recommendations and the Cybersecurity Analytics Support Team and their leadership has been working to enhance the program.

Recommendation 8: Update the Board's April 2018 guidance on the CER to clearly define the types of cybersecurity events that should be entered into the system.

By the end of 2021, we will update the CER (Cyber Event Repository) guidance to clearly define the types of events that should be entered into the system. The guidance will include information for users on the policy requirements for reporting cybersecurity events as well as the processes in place for inputting and submitting data into CER.

Recommendation 9: Develop instructions and training on the use of the CER, and issue guidance that requires CPCs (DSTs), or their designees, to complete this training.

By the end of 2021, we will develop instructions and training on reporting cybersecurity events and on using CER, aligned with the guidance above, which will be required for CPCs or their designees. We expect training to be completed within 6 months of the issuance of the guidance.

Recommendation 10: Update the cybersecurity incident playbook to reflect S&R's current organizational structure.

We are in the process of updating our incident playbook to reflect the changes in organizational structure. We plan to complete this revision by the end of June 2021.

The Division of Supervision and Regulation agrees with the conclusion of the report and we are developing full action plans to address the findings and recommendations, meeting the commitments contained within this response. As indicated in the title and body of the report, cybersecurity risks and supervision continues to evolve, as it should. To the extent the evolution impacts the planned actions to address recommendations, we will discuss planned changes with the OIG and how the recommendations will continue to be addressed.

Again, we appreciate the effort that went into this report and the guidance it provides as we continue to evolve and build our supervisory program for cybersecurity. This is a critical risk area for supervisors and the industry, and these recommendations serve to further enhance the quality and effectiveness of our program.

Regards,

Michael S. Gibson
Director
Division of Supervision and Regulation

Abbreviations

BTR	Business Technology Risk
CAST	Cybersecurity Analytics Support Team
CER	Cyber Event Repository
CPC	central point of contact
CPG	Cybersecurity Program Group
DST	dedicated supervisory team
FSOC	Financial Stability Oversight Council
G&C	governance and controls
GLBA	Gramm-Leach-Bliley Act
IT	information technology
LFI	large financial institution
LISCC	Large Institution Supervision Coordinating Committee
MAP	monitoring and analysis program
response guidance	*Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*
S&R	Division of Supervision and Regulation
security guidelines	*Interagency Guidelines Establishing Information Security Standards*
SORP	Systems and Operational Resiliency Policy

Report Contributors

Michael Zeitler, Project Lead and OIG Manager, Supervision and Regulation
Melissa Dorow, Auditor
Eric Shapiro, Auditor
Lindsay Taylor, Auditor
Corinne Torongo, Senior Auditor
Samuel Withers, Auditor
Daniel Novillo, OIG Manager, Supervision and Regulation
Laura Shakarji, Senior OIG Manager for Supervision and Regulation
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 Stop K-300
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 Stop K-300
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044