



Office of Inspector General

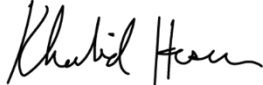
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: November 9, 2022

TO: Matthew J. Eichner
Director, Division of Reserve Bank Operations and Payment Systems
Board of Governors of the Federal Reserve System

Mark E. Van Der Weide
General Counsel
Board of Governors of the Federal Reserve System

FROM: Khalid Hasan 
Senior OIG Manager for Information Technology
Office of Information Technology

SUBJECT: OIG Memorandum Report 2022-IT-B-015: *Observations on Cybersecurity Risk Management Processes for Vendors Supporting the Main Street Lending Program and the Secondary Market Corporate Credit Facility*

Executive Summary

We are issuing this memorandum to communicate the results of our testing of the Main Street Lending Program (MSLP) and Secondary Market Corporate Credit Facility (SMCCF) cybersecurity vendor risk management processes. Overall, we found that MSLP and SMCCF officials worked closely with Federal Reserve System stakeholders, including Federal Reserve Bank information security officials, to quickly establish vendor contracts that generally met cybersecurity best practices. We also found that these officials took steps to evaluate the cybersecurity posture of vendors supporting these lending facilities. For example, vendors were required to complete an information security questionnaire as part of the procurement process.

We identified two ways in which third-party cybersecurity risk management processes can be strengthened for future scenarios: (1) include specific and measurable information security contract clauses and (2) use comprehensive vendor information security questionnaires. Additionally, we identified that Board of Governors of the Federal Reserve System and Reserve Bank information security program policy requirements for vendor risk management do not align.

This report does not contain recommendations.

Background

In response to the economic effects of the COVID-19 pandemic, the Board established several emergency lending programs and facilities to provide loans to employers, certain businesses, and communities across the country to support the U.S. economy.¹ The Coronavirus Aid, Relief, and Economic Security (CARES) Act authorizes the U.S. Department of the Treasury to invest in these facilities. Two of these facilities were the MSLP and the SMCCF.

MSLP

The Board established the MSLP to support lending to small and medium-sized for-profit businesses and nonprofit organizations across the United States.² A key purpose of the MSLP, which terminated on January 8, 2021, was to provide additional credit to assist companies that were in sound financial condition before the onset of the COVID-19 pandemic in maintaining their operations and payroll until conditions normalize. Specifically, the Board designed the MSLP to support small and medium-sized businesses that were unable to access the Paycheck Protection Program or that required additional financial support after receiving a Paycheck Protection Program loan.

The MSLP is administered by the Federal Reserve Bank of Boston (FRB Boston), which established a special purpose vehicle to purchase loan participations from eligible lenders across the United States. FRB Boston contracted with several vendors to provide support services for implementing and administering the MSLP, including the key vendors listed below as well as multiple legal services firms.³

- **State Street Bank and Trust Company:** State Street was retained on June 1, 2020, to serve as the custodian and accounting administrator for the MSLP.
- **Guidehouse Inc., working in partnership with PricewaterhouseCoopers LLP (Guidehouse-PwC):** Guidehouse-PwC was retained on June 14, 2020, to provide asset purchase intake, due diligence, and credit administration services for the MSLP. In addition, Guidehouse-PwC is responsible for developing and maintaining the MSLP's technology platform.
- **FTI Consulting, Inc.:** FTI Consulting was retained on March 1, 2021, to provide advisory-related and loan workout administration services for the MSLP.

SMCCF

The Board established the Primary Market Corporate Credit Facility (PMCCF) and the SMCCF (together, corporate credit facilities) to support credit to large employers. The PMCCF was designed to issue new bonds and loans.⁴ The SMCCF was designed to provide liquidity for outstanding corporate bonds. The

¹ The Board established these emergency lending facilities under section 13(3) of the Federal Reserve Act (12 U.S.C. § 343).

² The MSLP operated through five facilities: the Main Street New Loan Facility, the Main Street Expanded Loan Facility, the Main Street Priority Loan Facility, the Nonprofit Organization New Loan Facility, and the Nonprofit Organization Expanded Loan Facility.

³ FRB Boston posts quarterly reports to its public website on its use of vendors for the MSLP.

⁴ Because no transactions were made under the PMCCF while it was operational, there are no transaction-specific disclosures for that facility.

Federal Reserve Bank of New York (FRB New York) established one special purpose vehicle to manage and operate the corporate credit facilities, which ceased purchasing eligible assets on December 31, 2020.⁵ A key purpose of the SMCCF was to support market liquidity by purchasing, in the secondary market, corporate bonds issued by investment-grade U.S. companies as well as U.S.-listed exchange-traded funds whose investment objective is to provide broad exposure to the market for U.S. corporate bonds. Specifically, the Board designed the SMCCF to create a portfolio that tracked a broad, diversified market index of U.S. corporate bonds.

FRB New York contracted with several vendors to provide support services for implementing and administering the SMCCF, including the key vendors listed below as well as a legal service firm.⁶

- **BlackRock Financial Management, Inc.:** BlackRock was retained on March 24, 2020, to serve as the investment manager for the SMCCF. BlackRock also served as the cash investment manager for the SMCCF until February 2021, when it was replaced by Payden & Rygel.
- **State Street Bank and Trust Company:** State Street was retained on April 15, 2020, to serve as the custodian and accounting administrator for the SMCCF.
- **Payden & Rygel:** Payden & Rygel was retained on February 4, 2021, to serve as the cash investment manager for the SMCCF.

Objective, Scope, and Methodology

Our objective was to evaluate the effectiveness of (1) the risk management processes designed to ensure that effective information security and data integrity controls are implemented by third parties supporting the administration of the MSLP and SMCCF and (2) select security controls managed by the Reserve Banks for selected systems that process and maintain MSLP and SMCCF data.⁷ The scope of our evaluation included the key vendors supporting the administration of the MSLP and the SMCCF.⁸ Specifically, our scope included three third-party vendors for the MSLP—State Street, Guidehouse-PwC, and FTI Consulting—and three third-party vendors for the SMCCF—BlackRock, State Street, and Payden & Rygel.

To perform our testing, we reviewed the following for adherence to cybersecurity best practices: (1) evidence pertaining to the precontract due diligence performed, (2) the contracts and agreements in place, and (3) the ongoing postaward monitoring in place for each of the vendors included in our scope. Specifically, we reviewed contracts to determine whether security assurance language and requirements

⁵ On June 7, 2021, the SMCCF began winding down the portfolio and, as of August 31, 2021, all of its holdings of corporate bonds and exchange-traded funds had either matured or been sold.

⁶ FRB New York posts quarterly reports to its public website on its use of vendors for the SMCCF.

⁷ Given the timing of our testing and the operational status of the SMCCF, we decided not to perform security control testing for systems that process and maintain SMCCF data. Further, given the timing of testing and prior reviews of MSLP systems performed by FRB Boston general auditors, we decided not to perform security control testing for systems that process and maintain MSLP data.

⁸ As noted above, administration services include custodial and accounting, credit administration, loan workout, and investment management services.

were put in place for third-party vendors supporting the MSLP and the SMCCF in accordance with best practices. In addition, we reviewed documentation, such as *System and Organization Controls* reports and information security questionnaires, to determine whether due diligence and ongoing monitoring were performed in accordance with best practices.

Specifically, we reviewed the following best practices, which outline information security guidance that could be incorporated in vendor contracts:

- **U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*:** The standards state that management should incorporate methodologies for the acquisition of vendor packages into its information technology development.⁹ Additionally, management should design control activities over the selection, ongoing development, and maintenance of the agency's information technology, including vendor services and products.
- **Board Division of Information Technology, *Vendor Risk Management Standard*:** The standard defines security assurance requirements through each phase of the procurement process, as well as postaward continuous monitoring requirements. In addition, the Board has developed standard information security and cloud computing contract language to ensure that its security assurance and continuous monitoring requirements are enforceable.
- **National Institute of Standards and Technology (NIST), special publications (SPs):** NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, includes security requirements for the protection of federal information systems and data, such as media protection, incident reporting, user identification and authentication, record retention, and encryption of data at rest and in transit.¹⁰ NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, provides service requirement best practices for information technology decisionmakers using cloud computing technologies.¹¹
- **Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Cloud Computing Initiative:** The CIGIE Cloud Computing Initiative was intended to evaluate participating agencies' efforts when adopting cloud computing technologies and to review cloud service contracts for compliance with applicable standards. As part of this initiative, a checklist was developed to standardize agency responses and to determine whether agency contracts with cloud service providers contained clauses that align with relevant standards, for example, clauses related to access to cloud service provider facilities and specific details addressing investigative, forensic, and audit access.

⁹ U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.

¹⁰ National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, April 2013.

¹¹ National Institute of Standards and Technology, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, May 2012.

Our review of these best practices identified the following best practice categories: data protection, incident reporting, service-level requirements, user access, records management, and cooperation (table 1). We then used these categories to review the contract clauses.

Table 1. OIG-Determined Best Practice Categories

Area	Best practice	Reference
Data protection	Include clauses related to encryption, data location requirements, and how vendors monitor and control communications.	NIST SP 800-53: SC-7, SC-8, SC-13, SC-28, AU 10(5), MP-5(2)(4); Board <i>Vendor Risk Management Standard</i>
Incident reporting	Include clauses related to reporting and notification requirements for incidents or risk events.	NIST SP 800-53: IR-6, SI-5; Board <i>Vendor Risk Management Standard</i>
Service-level requirements	Include clauses related to service levels, such as uptime/downtime, monitoring responsibilities, remedy agreements, and amendments to service agreements.	NIST SP 800-146: 3.1 and 3.2
User access	Include clauses related to nondisclosure agreements, identifying and authenticating users, and personnel screening requirements.	NIST SP 800-53: IA-2(1)(2)(3)(8), IA-8, PS-3; Board <i>Vendor Risk Management Standard</i>
Records management	Include clauses related to the method of records management, including the timing of records destruction at the conclusion of the contract.	NIST SP 800-53: AU-11; Board <i>Vendor Risk Management Standard</i>
Cooperation	Include clauses related to access to the vendor’s facilities and records, as well as cooperation with auditors, law enforcement, and the Board.	CIGIE Cloud Computing Initiative

Source: OIG analysis of best practices.

We performed our fieldwork from June 16, 2021, through September 27, 2022. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Matter for Management Consideration: Third-Party Cybersecurity Risk Management Processes Can Be Strengthened

Overall, we found that MSLP and SMCCF officials worked closely with System stakeholders, including Reserve Bank information security officials, to quickly establish vendor contracts that generally met cybersecurity best practices. However, we found two areas in which the Board could work with FRB Boston and FRB New York to strengthen third-party cybersecurity risk management processes for future scenarios: (1) the inclusion of specific and measurable information security contract clauses and (2) the use of comprehensive vendor information security questionnaires.

In most of the contracts we reviewed, we found that while information security clauses were generally in line with best practices, contract clauses could have been stronger in several areas, such as incident response and records management.¹² For example, we noted that not all of the contracts identified specific time frames for incident notification or the return or destruction of Reserve Bank information at the end of the contract. FRB Boston officials informed us that vendors were hesitant to commit to specific time frames without knowing how large the MSLP would be; as such, incident response time frames were later clarified in vendor escalation procedures. These same officials also informed us that they now have a manager for MSLP vendors and that FRB Boston conducts periodic meetings with the vendors to update statements of work as needed. FRB New York officials informed us that some terms, such as specific incident response times, were removed during contract negotiation.¹³ In addition, each service provider agreement refers to information security questionnaires completed by the service provider, which FRB New York and FRB Boston considered as part of their due diligence.

However, we found that the majority of the information security questionnaires used by both FRB Boston and FRB New York did not cover the areas in the contracts that we identified for improvement. Specifically, while all vendors completed security questionnaires, we found that for five of the six vendors, FRB Boston and FRB New York used abbreviated information security control questionnaires. We understand this was done to facilitate the rapid onboarding of vendors to support MSLP and SMCCF operations. Further, FRB Boston and FRB New York officials informed us that full assessments were performed after the facilities were operational.¹⁴

We recognize that the Reserve Banks are not required to adhere to the best practices identified for the information security contract clauses we reviewed. Many MSLP vendors, however, will continue to

¹² Because of the sensitive nature of this information, we provided the details of our analysis in a separate restricted memorandum.

¹³ System officials noted that the vendor contracts included incident response provisions requiring vendors to provide notice “promptly,” which is an enforceable contract term.

¹⁴ The timing of our review did not allow us to verify the completion of these assessments.

provide services to the System and to the Board. We believe that if these clauses cannot be included in future contracts, management should ensure that they are included in the information security questionnaires completed by vendors as part of the due-diligence process.

Observation: The Vendor Cybersecurity Requirements of the Board and of the System Do Not Align

During our evaluation, we identified several inconsistencies between the vendor risk management policy requirements of the Board's information security program and of the System's Security Assurance for the Federal Reserve (SAFR), to which Reserve Banks are subject.¹⁵ For example, we noted that the vendor information security questionnaire used by the Board is generally more comprehensive than the SAFR vendor questionnaires used by FRB Boston and FRB New York.¹⁶ In addition, the Board has developed a standard information security clause that contains specific and measurable requirements, such as specific time periods for incident notification and the return or destruction of Board information at the end of the contract.¹⁷ SAFR policies do not require the inclusion of specific time frames. Further, depending on the information classification of the data maintained by the contractor, the Board's standard contract language includes requirements regarding the citizenship of contractor support staff or the geographic location of data or both; most of the MSLP and SMCCF contracts did not include such requirements.¹⁸

The *Board of Governor's Trust Model (BoG Trust Model)* is designed to document additional requirements that should be adopted by Reserve Bank systems that handle Board data to address differences in Board and SAFR security controls and supporting security program processes and activities. We noted, however, that the *BoG Trust Model* does not identify any differences between Board and SAFR policies for vendor risk management.

We were informed by Board and Reserve Bank stakeholders that the lending facility systems and vendors are not within the *BoG Trust Model's* scope; however, inconsistent Board and SAFR policies may affect other SAFR systems that maintain Board data. As such, we plan to perform follow-up work in this area as part of our future audit activities.

Closing

Our memorandum includes one matter for management consideration designed to strengthen third-party cybersecurity risk management processes in two areas: (1) the inclusion of specific and measurable

¹⁵ Both the Board, through the Board's information security program, and the System, through SAFR, have information security programs that provide a set of policies and controls to manage risk to the organization's information and information systems.

¹⁶ For example, we found that the Board's questionnaire included questions related to personnel security, including whether the vendor established specific screening criteria, whereas the questionnaire used by the Reserve Banks for five of the six lending facility vendors did not.

¹⁷ Whether to include the Board's standard information security clause on incident notification depends on the information classification of the information maintained by the vendor.

¹⁸ According to System officials, Reserve Banks cannot include citizenship requirements in contracts unless the work performed involves data from the U.S. Department of the Treasury or the Board. These same officials noted that these facilities did not include such data.

information security contract clauses and (2) the use of comprehensive vendor information security questionnaires. We believe that strengthening processes in these two areas could help ensure that vendors adhere to System and Board information security provisions when contractual relationships need to be established quickly.

We appreciate the cooperation that we received from Board, FRB Boston, and FRB New York officials during our review. Please contact me if you would like to discuss this memorandum or any related issues.

cc: Patrick J. McClanahan, Chief Operating Officer, Office of the Chief Operating Officer
Andreas Lehnert, Director, Division of Financial Stability
Trevor Reeve, Director, Division of Monetary Affairs
Stacey Tevlin, Director, Division of Research and Statistics
Ricardo A. Aguilera, Chief Financial Officer, Director, Division of Financial Management
Michelle A. Smith, Assistant to the Board, Chief of Staff, and Director, Division of Board Members
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Katherine Tom, Chief Data Officer, Office of the Chief Data Officer
Kenneth C. Montgomery, First Vice President and Chief Operating Officer, FRB Boston
Steven H. Wright, Senior Vice President and General Counsel, FRB Boston
Jon D. Colvin, Senior Vice President, General Auditor, FRB Boston
Anise Yi, Director, Audit, FRB Boston
Alicia R. Grasfeder, Assistant Vice President and Assistant General Auditor, Audit, FRB Boston
Daniel W. Hartman, Counsel, FRB Boston
Joe Lynch, Vice President, MSLP Operating Director, FRB Boston
Erin Boland, Assistant Vice President, Risk Management, MSLP, FRB Boston
Helen E. Mucciolo, First Vice President, Chief Financial Officer, Head, Corporate Group, FRB New York
Angela Sun, Assistant General Counsel, FRB New York
Meghan McCurdy, Assistant General Counsel, FRB New York
Andrew Danzig, Policy and Market Monitoring Advisor, FRB New York
Keith Pulsifer, Policy and Market Monitoring Advisor, FRB New York
Peter Seigel, Product Manager, FRB New York
Clive W. Blackwood, General Auditor, FRB New York
Ghada M. Ijam, System Chief Information Officer, FRB Richmond
Tammy Hornsby-Fink, Executive Vice President and Chief Information Security Officer, FRB Richmond
Jill Maier, Senior Manager, IT Business Services, FRB Richmond