OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

August 12, 2016

MEMORANDUM

TO: Distribution List

FROM: Peter Sheridan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report on the Board's Information Security Management Practices Pursuant to Section 406 of the Cybersecurity Act of 2015

The Office of Inspector General (OIG) is pleased to present its report on the information security management practices of the Board of Governors of the Federal Reserve System (Board), pursuant to section 406 of the Cybersecurity Act of 2015. Enacted into law on December 18, 2015, the act contains provisions meant to bolster cybersecurity protections at federal agencies, assess the federal government's cybersecurity workforce, and implement a range of measures intended to improve the cybersecurity preparedness of critical information systems and networks.

Section 406 of the act requires the OIG of each covered agency to submit a report on five information security areas related to the covered systems of the agency. The act defines a covered system as a national security system as described in 40 U.S.C. § 11103 or a federal computer system that provides access to personally identifiable information (PII). While the Board does not operate any national security systems, in order to meet its mission, the agency operates, manages, or relies on third parties for several systems that store, process, or transmit PII. As such, we address each of the five areas of the act below as it relates to these Board systems.

Since 2002, we have conducted annual audits of the Board's information security program, as required by the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA).[1] As such, we used our completed and ongoing information security audit work under FISMA as key inputs in developing this report. The work performed for this report was not conducted as an audit per *Government Auditing Standards*.

1. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-228, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–58).

1. Logical Access Policies and Practices

Section 406 of the Cybersecurity Act of 2015 requires the OIG to describe the logical access policies and practices used by the agency to access a covered system, including whether appropriate standards were followed. The Board has developed an information security program that includes policies and procedures that establish access controls to be implemented for all agency systems, including those covered by the act. These policies and procedures include roles and responsibilities for logical access controls and address control areas such as need to know, least privilege, rules of behavior, account management for general and privileged users, and access to portable and mobile devices. For instance, the Board's *Handling Personally Identifiable Information* policy states that only authorized users may access PII and that access must be limited to the minimum extent required to accomplish a job function.

The *Board Information Security Program* (BISP) and the Board's logical access policies and procedures for covered systems reference the Federal Information Processing Standards (FIPS), which are issued by the National Institute of Standards and Technology (NIST). These standards include

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- FIPS 140-2, *Security Requirements for Cryptographic Modules*

Our *2015 Audit of the Board's Information Security Program* found that the agency's information security program was generally consistent with FISMA requirements for identity and access management.[2] However, we identified several instances of sensitive information that was maintained in the Board's enterprise-wide collaboration tool that was not restricted to those with a need to know.

In addition, as part of our response to the U.S. Department of Homeland Security's FISMA reporting guidance for fiscal year 2015,[3] we noted that the Board had not implemented personal identity verification (PIV) cards for logical access to agency systems for general users. Implementation has been delayed due to technical difficulties and higher-priority projects. However, privileged users for the Board's Active Directory operating environment, which provides authentication services for the agency's network and several systems, including covered systems, authenticate using PIV-based multifactor authentication. Board officials noted that the

2. Office of Inspector General, *2015 Audit of the Board's Information Security Program,* OIG Report 2015-IT-B-019, November 13, 2015.

3. U.S. Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 19, 2015.

agency plans to transition all other administrators with access to covered systems to PIV-based multifactor authentication by the end of the third quarter of 2016.

Furthermore, in May 2016, we completed a security control review of the Board's Active Directory operating environment. Our review found that the Board could strengthen Active Directory controls in the areas of risk management, continuous monitoring, user group management, contractor account management, and system documentation.[4] We will evaluate the steps taken by the Board to strengthen the agency's identity and access management program as part of our ongoing 2016 FISMA audit of the agency's information security program.

2. Logical Access Controls and Multifactor Authentication for Privileged Users

Section 406 of the Cybersecurity Act of 2015 requires the OIG to provide a description and list of the logical access controls and multifactor authentication used by the agency to govern access to covered systems by privileged users. The Board uses a number of logical access controls, including multifactor authentication, to govern access to covered systems by privileged users. These include

- Usernames and passwords. Privileged users are required to enter usernames that follow Board-established naming standards and passwords that adhere to complexity, length, expiry, and history requirements. Passwords for privileged users must meet additional complexity requirements.

- Multifactor authentication. Remote access to the Board's network requires users to authenticate using a username, a password, and a token. The token includes a digital certificate that provides further authentication assurances. As noted above, privileged users for the Board's Active Directory operating environment, which provides authentication services for the agency's network and several applications, including covered systems, authenticate using PIV-based multifactor authentication. Board officials noted that the agency plans to transition all other administrators with access to covered systems to PIV-based multifactor authentication by the end of the third quarter of 2016. We are evaluating the Board's progress in this area as part of our ongoing 2016 FISMA audit of the agency's information security program.

- Rules of behavior. The Board requires all employees and contractors with access to agency information systems to be trained at least annually on the Board's rules of behavior. These rules include consequences for noncompliance with Board policies and procedures. The Board also requires system-specific rules of behavior to be developed and maintained.

- System timeouts. The Board requires system access timeouts due to inactivity to be implemented to protect access to all Board information resources.

4. Office of Inspector General, *Security Control Review of the Board's Active Directory Implementation*, OIG Report 2016-IT-B-008, May 11, 2016.

- Access reviews. The Board performs periodic access control reviews for its information systems to ensure that access is necessary and appropriate. The activities of privileged users must be reviewed more frequently.

- Audit logging. The Board requires several events to be logged and periodically reviewed for all agency systems, including privileged user logon and logoff, failed authentication attempts, and account management activities.

3. Reasons for Not Using Logical Access Controls or Multifactor Authentication

Section 225 of the Cybersecurity Act of 2015 directs agencies to implement multifactor authentication for remote access to information systems and for each account with elevated privileges on an agency information system by December 18, 2016. Section 406 of the act requires the OIG to describe the reasons the agency is not using logical access controls or multifactor authentication to govern access to covered systems by privileged users. As noted above, the Board uses various logical access controls to govern access to covered systems by privileged users. While the agency has implemented token-based multifactor authentication for remote access to its network, it is not currently using PIV or multifactor authentication for application-level access for general users. Also, as noted above, privileged users for the Board's Active Directory operating environment authenticate using PIV-based multifactor authentication.

Board officials noted that the agency plans to transition all other administrators with access to covered systems to PIV-based multifactor authentication by the end of the third quarter of 2016. Full implementation of PIV for general and privileged users has been delayed due to technical difficulties and higher-priority projects. Overall, the Board's planned activities for implementing PIV-based multifactor authentication are consistent with the requirements of section 225 of the act, and we will evaluate the Board's progress in this area as part of our ongoing 2016 FISMA audit of the agency's information security program.

4. Information Security Management Practices

a. Policies and Procedures to Inventory Software and Associated Licenses

Section 406 of the Cybersecurity Act of 2015 requires the OIG to describe the policies and procedures used to inventory software on the agency's covered systems as well as the licenses associated with the software. The BISP, in accordance with NIST guidance, requires system owners to develop, document, and maintain under configuration control a current baseline configuration of their covered systems. This configuration should include standard software packages installed on covered systems, current version numbers, and patch information on operating systems and applications. In addition, information system owners for all Board systems must develop a security plan that includes, among other things, the primary software used by the system. With respect to license management, Board officials informed us that the agency uses a combination of procurement and software management processes and tools to manage the licensing of software on covered systems.

As part of our 2015 FISMA audit of the Board's information security program, we noted that the Board cannot readily produce an accurate inventory of all the software installed on its network or the security configurations of all its software.[5] We will follow up on the status of the Board's efforts to address our recommendation in this area as part of our ongoing 2016 FISMA audit of the agency's information security program.

b. Monitoring and Detecting Data Exfiltration and Other Threats

Section 406 of the Cybersecurity Act of 2015 requires the OIG to describe the capabilities the agency uses to monitor and detect exfiltration and other threats, including data loss prevention (DLP) capabilities, forensics and visibility capabilities, or digital rights management (DRM) capabilities. The Board uses message classification and DLP systems, an enterprise incident response function with threat intelligence and forensics services, and a DRM solution in a limited capacity in order to monitor and detect data exfiltration and other threats.

c. How Monitoring and Detection Capabilities Are Used or Why They Are Not Used

Section 406 of the Cybersecurity Act of 2015 requires the OIG to describe how the agency uses capabilities to monitor and detect exfiltration and other threats, including DLP capabilities, forensics and visibility capabilities, or DRM capabilities. The act also requires the OIG to describe the reasons why the agency may not be using such capabilities. The Board uses a client-based DLP solution to identify when classified information, including PII, is being sent to an external email address, copied to an unauthorized storage device, or posted to an external website. In addition, to decrease the risk of accidental loss, the Board has implemented email rules that require users to explicitly state that they want to send an email to an external user. All emails sent from a desktop, laptop, or tablet are required to have information classification and delivery designations selected.

The Board also uses the services of a Federal Reserve Systemwide incident response function for threat intelligence, incident response, and forensics services. In addition, the Board uses a DRM solution in a limited capacity to control access to its most sensitive electronic documents, such as those dealing with Federal Open Market Committee actions.

5. Policies and Procedures to Ensure Contractors and Other Service Providers Implement Information Security Management Practices

Section 406 of the Cybersecurity Act of 2015 requires the OIG to describe the policies and procedures of the agency with respect to ensuring that entities, including contractors providing services to the agency, are implementing the information security management practices described in this report. The Board's information security policies and procedures apply to all

5. Office of Inspector General, *2015 Audit of the Board's Information Security Program*, OIG Report 2015-IT-B-019, November 13, 2015.

systems, including those operated for or on behalf of the Board by contractors or other organizations.

To ensure that third-party contractors are implementing the information security management practices described in this report, the Board has established a third-party review process that addresses the majority of NIST-recommended security controls. The process includes questionnaires that are a part of all requests for proposal, and these questionnaires are used by the Board to determine a security risk level for third-party systems. The security risk level drives the level of assurance that is required during security reviews as well as the frequency of monitoring activities. In addition, security assessments are required to be completed for all third-party systems.

The Board also uses covered systems that are operated or maintained by the Federal Reserve Banks. The Reserve Banks are classified as external entities with respect to FISMA. As part of our security control reviews, we identified improvements needed in the Board's oversight processes to ensure that security controls provided by Federal Reserve Bank service providers meet Board security requirements.[6]

The Board is currently evaluating the Federal Reserve System's information security program and review processes to ensure that they align with the requirements of the BISP. The Board anticipates developing a trust agreement at the conclusion of that analysis. As part of our ongoing 2016 FISMA audit of the agency's information security program, we plan to evaluate the steps taken by the Board to strengthen its processes to ensure that all third-party systems meet FISMA and Board information security requirements.

Closing

We are currently conducting our 2016 audit of the Board's information security program, as required by FISMA. This ongoing audit will include an overall assessment of the effectiveness of the Board's policies, procedures, and controls in the security areas described above. Our FISMA audit report will incorporate information contained in this report and will be available on our public website in mid-November 2016 to meet the FISMA reporting deadline established by the U.S. Department of Homeland Security.

We appreciate the cooperation we received from Board officials during our review. Please contact me at 202-973-5009 if you would like to discuss this report or any related issue.

6. Office of Inspector General, *Security Control Review of the Board's Statistics and Reserves System*, OIG Report 2015-IT-B-021, December 17, 2015.

cc: William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Scott G. Alvarez, General Counsel, Legal Division
Linda Robertson, Assistant to the Board for Congressional Relations, Office of Board Members
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General
Jacqueline Becker, Associate Inspector General for Legal Services and Counsel to the Inspector General

Distribution:
Donald V. Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Raymond Romero, Chief Privacy Officer, Division of Information Technology
Charles Young, Chief Information Security Officer, Division of Information Technology