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 CFPB'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 Consumer Financial Protection Bureau (CFPB), 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 CFPB 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 as it relates to these CFPB systems.

Since the CFPB became fully operational in July 2011, we have conducted annual audits of the agency'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 for 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 CFPB's information security program includes policies and procedures that establish logical access controls to be implemented for all CFPB systems, including those covered by the act. These policies and procedures include roles and responsibilities and address control areas such as need to know, least privilege, rules of behavior, account management for general and privileged users, remote/virtual private network access, and access to portable and mobile devices. For example, the CFPB's information security guidance notes that all users are to be given access to only those systems and information that they require to perform their jobs. Users must complete an approval process prior to being granted access to PII.

The CFPB's information security program and logical access policies and practices reference various federal guidance documents and standards, including the Federal Information Processing Standards (FIPS), which are issued by the National Institute of Standards and Technology. 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 140-2, *Security Requirements for Cryptographic Modules*

In 2015, we reported that the agency's information security program was generally consistent with FISMA requirements for identification and authentication.[2] However, we noted that the CFPB was not regularly reviewing and updating several of its policy, procedure, standard, and process documents, including those for logical access for all of the agency's systems. Our ongoing 2016 FISMA audit of the CFPB's information security program will include an assessment of the steps taken by the agency to address this issue. We will also evaluate the progress made by the agency in strengthening its identity and access management program and access controls for select systems.

Further, while the CFPB uses multifactor, token-based authentication for remote access to the agency's network, it has not implemented personal identity verification (PIV) cards for logical access to the agency's network and systems. CFPB officials noted that the agency is making progress in implementing PIV; however, implementation has been delayed due to the prioritization of competing initiatives and the timing of the agency's transition from the U.S. Department of the Treasury's (Treasury) technology infrastructure to its own.

The OIG also has an ongoing audit of the CFPB's Active Directory operating environment, which provides the logical access controls for the agency's network and specific applications.

2. Office of Inspector General, *2015 Audit of the CFPB's Information Security Program*, OIG Report 2015-IT-C-020, November 13, 2015.

This audit includes a review of logical access processes, the results of which will be incorporated into our 2016 audit of the CFPB's information security program, as required by FISMA.

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 covered agency to govern access to covered systems by privileged users. The CFPB uses a number of logical access controls and multifactor authentication to govern access to covered systems by privileged users. These include

- Usernames and passwords. Usernames for all CFPB users, including privileged users, are required to follow CFPB-established naming standards, and all passwords must adhere to complexity, length, and age requirements.

- Multifactor authentication. All users, including privileged users, accessing CFPB covered systems remotely through a virtual private network must use a token in conjunction with a username and a complex password to provide two-factor authentication.

- Rules of behavior. All users of the CFPB's network are required to acknowledge the CFPB's acceptable use policy, which specifies the rules and expectations of conduct and behavior while using CFPB information resources. In addition, the CFPB requires all privileged users to review and acknowledge rules of behavior specific to that role before being granted elevated privileges. These rules cover protection of passwords and other authentication credentials, reporting of security incidents, and use of a PIV or a Level of Assurance 4 credential when such credentials are available.[3] The need for privileged access must be validated by management at least once a year, at which point the elevated privileges are reauthorized or revoked.

- System timeouts. The CFPB requires system access timeouts due to inactivity to be implemented, where technically feasible, to protect access to all CFPB information resources.

- Access reviews. The CFPB's information systems security managers and information systems security officers are required to perform periodic audits of systems under their purview to review privileged user access.

- Audit logging. The CFPB requires specific system and security events to be logged and periodically reviewed for all agency systems, including, but not limited to, all privileged user actions related to system and security administration.

3. OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, defines four levels of assurance, levels 1-4, in terms of the consequences of authentication errors and the misuse of credentials. Level 1 is the lowest assurance level, and level 4 is the highest.

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

Section 406 of the Cybersecurity Act of 2015 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 CFPB uses various logical access controls to govern access to covered systems by privileged users. While the agency has implemented multifactor authentication for remote access to its network, it is working to implement multifactor authentication for all covered systems.

During its first four years, the CFPB prioritized establishing core business technology capabilities and transitioning its wide area network and remote access infrastructure from Treasury. With this transition completed in 2015, the CFPB can prioritize the implementation of an identity and access management solution that includes multifactor authentication for all covered systems.

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 such software. The CFPB's information security policy requires system owners to ensure the development of baseline information for all agency systems, including a current list of all system components (hardware, software, and documentation) and version releases for all software. In addition, all CFPB systems must be covered by a system security plan that includes, among other things, the primary software used by the system.

In conducting our FISMA work, we have found that the CFPB performs periodic automated vulnerability scanning on its systems to gather inventory, configuration, and vulnerability data. Further, the agency uses system configuration and network management tools to inventory software on its systems.

With respect to license management, CFPB officials informed us that the agency uses automated tools to manage the software licenses of the most common commercial software products used at the agency. For other software types, spreadsheets are used to track the status of licenses. Inventories are performed by comparing the licensed instance lists against the licenses that are in operation on the systems employed at the CFPB and by performing causative research to address any discrepancies.

As part of our 2013 FISMA audit, we recommended that the CFPB develop and implement an agency-wide configuration management plan.[4] Such a plan would provide a comprehensive description of the roles, responsibilities, policies, and procedures when managing the

4. Office of Inspector General, *2013 Audit of the CFPB's Information Security Program*, OIG Report 2013-IT-C-020, December 2, 2013.

configuration of information systems, including software. The CFPB recently finalized its plan, and we are evaluating its effectiveness as part of our ongoing 2016 FISMA audit of the CFPB'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 CFPB uses a U.S. Department of Homeland Security–approved Managed Trusted Internet Protocol Service (MTIPS) provider for monitoring and detecting exfiltration and other threats at the agency's network perimeter. The agency has also deployed intrusion detection systems at its major network access points and is in the process of implementing an automated solution to perform centralized monitoring and incident correlation functions.

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 CFPB has established a Computer Security Incident Response Team (CSIRT) whose mission is to monitor, detect, prevent, and respond to cybersecurity incidents for agency systems, users, and information technology services through distributed defenses, threat detection and mitigation, and response capabilities. The CSIRT works with other technology operations teams at the CFPB and coordinates with the agency's MTIPS provider as needed to monitor and protect the agency's information resources. In carrying out its mission, the CSIRT analyzes various sources of information, including, but not limited to, intrusion detection and prevention alerts, audit and activity logs, network data, intelligence reporting, and third-party external notifications, such as from intelligence and counterintelligence sources.

As part of our 2013 FISMA audit, we recommended that the CFPB ensure that audit logs and security incident information from all relevant sources are centrally tracked, analyzed, and correlated.[5] In 2014, we found that the CFPB was in the process of procuring an automated tool to provide these capabilities.[6] In 2015, we found that the CFPB had selected and procured an automated tool and was configuring it for deployment.[7] Our ongoing 2016 FISMA audit of the

5. Office of Inspector General, *2013 Audit of the CFPB's Information Security Program*, OIG Report 2013-IT-C-020, December 2, 2013.

6. Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*, OIG Report 2014-IT-C-020, November 14, 2014.

7. Office of Inspector General, *2015 Audit of the CFPB's Information Security Program*, OIG Report 2015-IT-C-020, November 13, 2015.

CFPB's information security program will include an assessment of the CFPB's progress in implementing its selected automated tool in this area.

Also as part of our ongoing 2016 FISMA audit, we found that the CFPB uses the DLP services provided by its MTIPS network provider to monitor and detect threats at its external network boundary. With the transition of its information technology infrastructure from Treasury completed, and as part of a defense-in-depth approach, the agency is prioritizing the implementation of a DLP program for its internal network. Agency officials noted that the DLP program will include the development of policies and procedures, implementation of DLP technologies, and user training. Further, the CFPB obtains forensic analysis services through contracted service providers or in coordination with the OIG, as needed. CFPB officials also informed us that the agency has put an electronic discovery (e-discovery) process and tool set into operation and that it has e-discovery specialists on staff.

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 covered 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 CFPB's information security policies and procedures apply to all systems, including those operated for or on behalf of the CFPB by contractors or other organizations. To ensure that entities, including contractors, are implementing the information security management practices described in this report, the CFPB has developed a third-party risk assessment process that includes activities for identifying, assessing, and mitigating risks. In addition, the CFPB reviews contracts with third-party providers to ensure that the requisite clauses are included related to the information security management practices discussed in this report.

We have identified ensuring the security of contractor-operated information systems as a management challenge facing the CFPB.[8] Specifically, the CFPB relies on a variety of contractor-operated and contractor-maintained systems to meet its mission, including several cloud computing–based systems in which computing resources may be shared with other federal or commercial entities. In January 2014, we conducted an audit to review the CFPB's acquisition and contract management for select cloud computing–based systems. Our objective was to determine whether requirements for security, service levels, and access to records were appropriately planned for, defined in contracts, and monitored.

We found that the CFPB had established a process to monitor both contractual and service-level requirements for its cloud providers. However, we identified, among other things, opportunities to strengthen the CFPB's procurement processes to ensure that its contracts with service

8. Office of Inspector General, *2015 List of Major Management Challenges for the CFPB*, September 30, 2015.

providers include best practice contract clauses for e-discovery and forensic investigations.[9] Since the completion of our audit, CFPB officials informed us that actions have been taken to ensure that future contract revisions include the appropriate clauses. As part of our ongoing 2016 FISMA audit, we plan to evaluate the steps taken by the CFPB to strengthen its processes to ensure that contractor systems meet FISMA and CFPB information security requirements.

Closing

We are currently conducting our 2016 audit of the CFPB's information security program, as required by FISMA. This ongoing audit will include an overall assessment of the effectiveness of the CFPB'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 CFPB officials during our review. Please contact me at 202-973-5009 if you would like to discuss this report or any related issue.

cc: Stephen Agostini, Chief Financial Officer and Assistant Director, Office of the Chief Financial Officer
Mary McLeod, General Counsel
Zixta Martinez, Associate Director, Division of External Affairs
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:
Sartaj Alag, Chief Operating Officer and Associate Director, Division of Operations
Vijay Desai, Acting Chief Information Officer and Acting Assistant Director, Technology and Innovation
Claire Stapleton, Chief Privacy Officer
Zachary Brown, Chief Information Security Officer

9. Office of Inspector General, *2013 Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services*, OIG Report 2014-IT-C-016, September 30, 2014.