BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
BUREAU OF CONSUMER FINANCIAL PROTECTION

Consumer Financial Protection Bureau

OFFICE OF INSPECTOR GENERAL

November 15, 2011

Mr. Chris Willey
Chief Information Officer
Bureau of Consumer Financial Protection
Washington, D.C. 20220

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the Bureau of Consumer Financial Protection (CFPB), to develop, document, and implement an agency-wide information security program. FISMA also requires each Inspector General (IG) to conduct an annual independent evaluation of its agency's information security program and practices, to include testing controls for a subset of systems. The CFPB is relying on the information security program and computer systems of the Department of the Treasury (Treasury). As part of its 2011 FISMA audit, the Treasury Office of Inspector General (OIG) evaluated the effectiveness of Treasury's information security programs, including controls for 15 systems across Treasury bureaus. One of the systems included in the Treasury OIG's FISMA review was a general support system that the CFPB is relying on for network infrastructure and connectivity to support a number of applications. To meet our annual FISMA reporting responsibilities for the CFPB and avoid duplication of effort, we relied on the FISMA work performed by the Treasury OIG. Appendix 1 summarizes the results of the Treasury OIG's FISMA review, as it pertains to Treasury's information security program and the general support system on which the CFPB is relying.

The Treasury OIG contracted with KPMG LLC, an independent certified public accounting firm, to perform its 2011 FISMA audit. Overall, KPMG concluded that Treasury's information security program and practices for its non-Internal Revenue Service (IRS) bureaus' unclassified systems were generally consistent with the requirements of FISMA. KPMG noted, however, that "Treasury's information security program was not fully effective," as evidenced by control weaknesses identified for various Treasury systems.[1] Treasury can improve the effectiveness of its information security program and controls for the general support system that CFPB relies on by strengthening risk management, configuration management, and contingency planning controls.

As part of an agency's annual FISMA reporting, the Department of Homeland Security (DHS) requests that both the Chief Information Officer (CIO) and IG perform an analysis of certain agency information security program components.[2] For IGs, these components include risk management, continuous monitoring, security configuration management, security training, contractor oversight, contingency planning, incident response and reporting, and security capital

[1] KPMG LLC's Fiscal Year 2011 FISMA Performance Audit of The Department of the Treasury (November 2011).

[2] DHS Federal Information Security Memorandum 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (August 24, 2011).

planning. Our responses to DHS's questions in these areas will be transmitted under separate cover and will reflect KPMG's findings for Treasury's information security program and the general support system CFPB relies on. CFPB officials informed us that, in consultation with DHS, CFPB, as a recently established federal agency, will start reporting on these components during the second quarter of fiscal year 2012.

We provided a draft of this report to the CFPB CIO, and his response is included as appendix 2. In his response, the CIO stated that the CFPB continues to leverage certain services provided by Treasury as an interim means to maintain operational efficiencies. The CIO also noted that a key component of CFPB technology independence is a robust and comprehensive cybersecurity program. The CFPB's cybersecurity program is aligned to the risk management framework developed by the National Institute of Standards and Technology (NIST). As a newly established agency, the CFPB is working steadily to develop and mature its internal functions and processes to include the many facets of technology management.

This report will be added to our publicly available web site and will be summarized in our next semiannual report to Congress. We appreciate the cooperation we received from the CFPB and Treasury during our review. We will continue to monitor and report on the CFPB's efforts in establishing an information security program as part of our responsibilities under FISMA. Please contact me at 202-973-5003 if you would like to discuss this report or any related issues.

Sincerely,

Andrew Patchan Jr.
Associate Inspector General for Audits and Attestations

cc: Catherine West, Chief Operating Officer, CFPB
Zachary Brown, Acting Chief Information Security Officer, CFPB
Marla A. Freedman, Assistant Inspector General for Audit, OIG, Treasury

APPENDIXES

This appendix summarizes the results of the Treasury OIG's FISMA review, as it pertains to Treasury's information security program and the general support system on which the CFPB relies.

BACKGROUND

FISMA provides a framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[3] FISMA requires federal agencies, including the CFPB, to develop, document, and implement an agency-wide information security program. This program is to provide security for the information and information systems of the agency, including those provided by another agency, contractor, or other source. FISMA further requires each agency IG to perform an annual independent evaluation of its agency's information security program and practices, to include testing controls for a subset of systems.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) established the CFPB as an independent and autonomous entity within the Federal Reserve System.[4] Under Dodd-Frank, the CFPB is charged with ensuring that markets for consumer financial products and services are fair, transparent, and competitive. Dodd-Frank assigned the responsibility for performing certain CFPB functions to the Secretary of the Treasury until a Director for the CFPB is in place.[5] In addition, Dodd-Frank established our office as the IG for the CFPB.

The CFPB relies on and is leveraging Treasury's Departmental Offices' (DO's) information security program, policies, procedures, and systems until it matures as an organization and can perform these functions on its own. DO, while not an operating bureau of Treasury,[6] consists of offices that are primarily responsible for the formulation of policy and Treasury-wide management issues, including the provision of information technology and administrative support to Treasury bureaus. With respect to FISMA, Treasury has established overall department-wide information security policies, and each Treasury bureau and DO operate and maintain their own information security program. The CFPB entered into an agreement with DO for the provision of administrative services, including facilities, computer systems, and information security.

The Treasury OIG, as part of its responsibilities under FISMA, performs an annual independent evaluation of Treasury's information security program and controls for select systems. The Treasury OIG contracted with KPMG LLP, an independent certified public accounting firm, to perform its 2011 FISMA evaluation. To perform this evaluation, KPMG evaluated the policies and procedures established for Treasury's information security program and those established for

[3] Title III, Pub. L. No. 107-347 (December 17, 2002).
[4] Title X, Pub. L. No. 111-203 (July 21, 2010).
[5] As of the date of this report, a Director for the CFPB has not been confirmed by the Senate.
[6] Treasury consists of the following 12 operating bureaus: Alcohol and Tobacco Tax and Trade; Engraving and Printing; Public Debt; Community Development Financial Institution Fund; Financial Crimes Enforcement Network; Financial Management Service; Inspector General; Treasury Inspector General for Tax Administration; Internal Revenue Service; Office of the Comptroller of the Currency (OCC); Office of Thrift Supervision (OTS); and U.S. Mint. As a result of Dodd-Frank, the functions of OTS were transferred to the Board of Governors of the Federal Reserve System, the OCC, and the Federal Deposit Insurance Corporation effective July 21, 2011.

Treasury's operating bureaus and DO. KPMG also tested controls for select systems across Treasury's bureaus and DO, including a DO general support system that the CFPB relies on to support a number of applications. This general support system provides the CFPB with the network infrastructure, including routers, firewalls, and other security devices, needed to access the Internet and connect with various Treasury systems. This system also supports the desktop and laptop computers that CFPB employees utilize.

OBJECTIVES, SCOPE, AND METHODOLOGY

KPMG reported that its objectives for its 2011 FISMA audit of Treasury were to determine the effectiveness of Treasury's information security programs and practices for the period July 1, 2010, to June 30, 2011, for Treasury's unclassified systems. This included a determination as to whether non-IRS Treasury bureaus had implemented (1) an information security program, consisting of policies, procedures, and security controls consistent with the FISMA legislation; and (2) the security controls catalog contained in NIST Special Publication (SP) 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*. To meet our FISMA reporting responsibilities for the CFPB and to avoid duplication of effort, we relied on the work performed by KPMG as part of its 2011 FISMA audit of Treasury. Specifically, we relied on the work performed by KPMG with respect to its evaluation of DO's information security program and controls for a DO general support system that the CFPB utilizes.

KPMG reported that it conducted its FISMA audit of Treasury's information security program in accordance with generally accepted government auditing standards (GAGAS). Those standards require KPMG to plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. To meet GAGAS requirements for relying on the work of others, we performed appropriate procedures, including

- Obtaining evidence on the qualifications and independence of KPMG staff performing the FISMA audit of Treasury;
- Reviewing Treasury OIG's FISMA audit plan, KPMG's audit report, and KPMG's workpaper documentation;
- Meeting with Treasury OIG officials to gain an understanding of how they perform their FISMA oversight of Treasury's information security program, including reviewing the work performed by KPMG; and
- Discussing KPMG's audit approach and results with KPMG staff.

Our audit scope was focused on summarizing the work KPMG performed with respect to its review of DO's information security program and controls for the DO general support system that CFPB utilizes. We also utilized KPMG's results for their review of DO's information security program and controls for the DO system to respond to specific questions that DHS has requested IGs to address in their 2011 FISMA reporting. We will provide our analysis of DHS's specific questions under separate cover. Our scope did not include an evaluation of all the work KPMG performed as part of its overall FISMA audit of Treasury's information security program. We also did not analyze information technology that CPFB is developing beyond what is provided by Treasury and reviewed by KPMG in 2011.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Overall, KPMG concluded that Treasury's information security program and practices for its non-IRS bureaus' unclassified systems were generally consistent with the requirements of FISMA. KPMG also concluded that DO had established and implemented an information security program, common security policies, and procedures based on NIST and Treasury guidelines. KPMG noted, however, that Treasury's, including DO's, information security programs "were not fully effective," as evidenced by control weaknesses identified for various Treasury systems. With regard to the DO general support system that CFPB relies on, KPMG reported the following two findings and associated recommendations, in support of its conclusion that Treasury's, including DO's, information security program was not fully effective.

- The system security plan did not include all required security controls as specified in NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009. To address this finding, KPMG recommended that DO management instruct the vendor operating the general support system to update the system security plan to include NIST SP 800-53, Rev. 3 security controls and associated control enhancements.

- High risk vulnerabilities identified in a vulnerability scan report for the DO general support system were not remediated within 30 days, as required. To address this finding, KPMG recommended that DO management direct personnel charged with remediating vulnerabilities to track open, unresolved vulnerabilities in system plans of actions and milestones when the anticipated remediation will exceed 30 days.

KPMG also identified two additional control deficiencies for the DO general support system on which CFPB relies. KPMG did not classify these as findings, since DO management had already identified these weaknesses and had identified corrective actions to address them. These control deficiencies were (1) the Federal Desktop Core Configuration standard was not implemented for desktop computers and a waiver was not obtained to implement a different standard; and (2) a backup process for configuration files residing in firewalls, intrusion prevention systems, routers, and switches had not been established.

APPENDIX 2

Chief Information Officer's Comments

cfpb Consumer Financial Protection Bureau

1500 Pennsylvania Ave, NW (Attn: 1801 L St)
Washington, DC 20220

November 15, 2011

MEMORANDUM FROM: CHRIS WILLEY
CHIEF INFORMATION OFFICER
CONSUMER FINANCIAL PROTECTION BUREAU

SUBJECT: Response to FISMA 2011 Memorandum from the Board of Governors of the Federal Reserve System Bureau of Consumer Financial Protection

Under the provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the Department of the Treasury was charged with providing various administrative functions to support the stand-up of the Consumer Financial Protection Bureau (CFPB). The CFPB continues to leverage certain commodity services provided by the Department as an interim means to maintain operational efficiencies. Among those Department services is the information technology system referenced in this memorandum.

As a newly established agency, the CFPB is working steadily to develop and mature its internal functions and processes to include the many facets of technology management. While operating on the Treasury IT infrastructure, the CFPB is afforded the opportunity to plan and design an IT infrastructure that can support the CFPB mission well into the future. The guiding principle of achieving efficiency and excellence through strategic technology decisions is helping to shape the systems and infrastructure of the independent CFPB.

A key component of CFPB technology independence is a robust and comprehensive Cybersecurity program that complies with FISMA. The CFPB Cybersecurity program is aligned to the Risk Management Framework (RMF) as prescribed by the National Institute of Standards and Technology (NIST) which calls for transparency and reciprocity between organizations with regard to security assessments and authorizations. The CFPB will promote and rely on these concepts to achieve efficiencies and excellence in risk management. The CFPB will continue to work closely with the Department of the Treasury to ensure that third-party risk to the CFPB operating environment has been accounted for and mitigated accordingly.