REDACTED

Federal Housing Finance Agency
Office of Inspector General

Kearney & Company, P.C.'s Results of the Federal Housing Finance Agency's Cybersecurity Act Audit

Audit Report • AUD-2016-004 • August 11, 2016

OFFICE OF INSPECTOR GENERAL

Federal Housing Finance Agency

400 7th Street SW, Washington, DC 20219

August 11, 2016

TO: Kevin Winkler
Chief Information Officer

FROM: Marla A. Freedman /s/
Deputy Inspector General for Audits

SUBJECT: Audit Report – *Kearney & Company, P.C.'s Results of the Federal Housing Finance Agency's Cybersecurity Act Audit*

We are pleased to transmit the subject report.

Section 406 of the Cybersecurity Act of 2015, enacted as Division N of the Consolidated Appropriations Act, 2016, December 18, 2015,[1] requires the Federal Housing Finance Agency (FHFA) Inspector General to report to Congress the following information to be collected from FHFA on FHFA computer systems that provide access to personally identifiable information (PII): (a) a description of the logical access policies and practices used to access a PII system, including whether appropriate standards were followed; (b) a description and list of the logical access controls and multi-factor authentication used by the agency to govern access to PII systems by privileged users; (c) a description of policies and procedures followed to detect data exfiltration and maintain an inventory of software and licenses on the covered systems; and (d) a description of policies and procedures to ensure that contractors and other entities providing services to the agency implement appropriate data security management practices.

We contracted with the independent certified public accounting firm of Kearney & Company, P.C. (Kearney) to conduct a performance audit to meet this reporting requirement. The contract required that the audit be conducted in accordance with generally accepted government auditing standards.

In its audit, Kearney concluded FHFA has established and implemented the required privacy controls according to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for "moderate" impact systems as of June 30, 2016. Additionally, FHFA has satisfied the NIST SP 800-53 required privacy controls for six reviewed systems and has implemented a combination of preventive and detective security controls (e.g., network firewalls, encryption, intrusion detection systems, etc.) to protect sensitive information such as PII.

[1] Public Law 114-113.

In connection with the contract, we reviewed Kearney's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to conclude, and we do not conclude, on FHFA's compliance with required privacy controls according to NIST SP 800-53. Kearney is responsible for the attached auditor's report dated August 11, 2016, and the conclusions expressed in the report. However, our review found no instances where Kearney did not comply, in all material respects, with generally accepted government auditing standards.

Report Distribution

Federal Housing Finance Agency

Director
Chief of Staff
Chief Operating Officer
Chief Financial Officer
Chief Information Officer
Internal Controls and Audit Follow-up Manager

Office of Management and Budget

Budget Examiner

United States Senate

Chair and Ranking Members

Committee on Appropriations, Subcommittee on Transportation, Housing and Urban Development, and Related Agencies

Committee on Banking, Housing, and Urban Affairs

Committee on Homeland Security and Governmental Affairs

U.S. House of Representatives

Chair and Ranking Members

Committee on Appropriations, Subcommittee on Transportation, Housing and Urban Development, and Related Agencies

Committee on Financial Services

Committee on Oversight and Government Reform

Federal Housing Finance Agency
Office of Inspector General

Results of FHFA's Cybersecurity Act of 2015 Audit

August 11, 2016

Point of Contact:
Tyler Harding, Principal
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
Tyler.Harding@kearneyco.com
Kearney & Company's TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14

TABLE OF CONTENTS

ACRONYM LISTING

Acronym	Definition
AD	Active Directory
COTS	Commercial Off-the-Shelf
CSA	Cybersecurity Act of 2015
CTS	Correspondence Tracking System
DLP	Data Loss Prevention
DRM	Digital Rights Management
EEX	Employee Express
Fannie Mae	Federal National Mortgage Association
FHFA	Federal Housing Finance Agency
FHFB	Federal Housing Finance Board
FHLBanks	Federal Home Loan Banks
FHR	Federal Human Resources
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
Freddie Mac	Federal Home Loan Mortgage Corporation
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
HERA	Housing and Economic Recovery Act of 2008
iComplaints	MicroPact iComplaints
ID	Identification
IT	Information Technology
JPP	Job Performance Plan
Kearney	Kearney & Company, P.C.
NIST	National Institute of Standards and Technology
N/A	Not Applicable
OFHEO	Office of Federal Housing Enterprise Oversight
OIG	Office of Inspector General
OHRM	Office of Human Resources Management
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OTIM	Office of Technology and Information Management
P.L.	Public Law
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
POA&M	Plans of Action and Milestones

Acronym	Definition
PUB	Publication
Rev.	Revision
SA&A	Security Assessment and Authorization
SAR	Security Assessment Report
SORN	Systems Of Records Notice
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan
U.S.	United States

KEARNEY&
COMPANY

COVER LETTER
August 11, 2016

The Honorable Laura S. Wertheimer
Inspector General
Federal Housing Finance Agency
400 7th Street SW
Washington, D.C. 20024

Dear Inspector General Wertheimer:

Kearney & Company, P.C. (defined as "Kearney," "we," and "our" in this report) is pleased to provide this Cybersecurity Act of 2015 (CSA) Audit Report, which details the results of our audit of the Federal Housing Finance Agency's (FHFA or Agency) implementation of specific security and privacy controls as directed by Section 406, *Federal Computer Security*, of the CSA. Section 406 requires the FHFA Inspector General to report on FHFA's logical access controls, data exfiltration protections, and other policies and procedures governing the protection of personally identifiable information (PII) data within covered systems.[2] The FHFA Office of Inspector General (OIG) contracted with Kearney to conduct this independent audit as a performance audit under generally accepted government auditing standards (GAGAS).

The objective of this audit was to report information to the United States Congress detailing FHFA's establishment and implementation of logical access, software management, and data exfiltration controls on covered systems. Kearney's methodology for the FY 2016 CSA evaluation included an assessment of six FHFA information systems for compliance with selected controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, found in Appendix J: *Privacy Control Catalog*.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[2] The CSA defines a "covered agency" as an agency operating a covered system. A "covered system" refers to a national security system as defined in Section 11103 of Title 40, United States Code (U.S.C.), or a Federal computer system that provides access to PII. The full text is available at https://www.congress.gov/bill/114th-congress/house-bill/2029/text in Division N. (Accessed by Kearney July 22, 2016)

Based on our audit work, we concluded that FHFA has established and implemented the required privacy controls according to NIST SP 800-53 for "moderate" impact systems as of June 30, 2016. In particular, strengths of the Privacy Program included the following:

1. Completed and published system of record notices (SORN) and privacy impact assessments for the six sampled information systems
2. Evidence of oversight for third-party information systems containing PII
3. Inclusion of privacy-based requirements in contracts with service providers
4. Privacy monitoring and auditing of privacy-related controls
5. Privacy awareness and training.

FHFA has satisfied the NIST SP 800-53 required privacy controls for the six reviewed systems and has implemented a combination of preventive and detective security controls (e.g., network firewalls, encryption, intrusion detection systems, etc.) to protect sensitive information such as PII. We encourage FHFA to continue to evaluate technical solutions promoted by the CSA, such as data loss prevention tools to strengthen FHFA's protection of privacy data over its covered systems. Detailed observations are included in the *Results* section of this report. The projection to future periods of any conclusions based on our findings is subject to the risk that controls may become inadequate due to changes in conditions or the deterioration of compliance with controls.

In closing, we appreciate the courtesies extended to the Kearney Audit Team by FHFA during this engagement.

Sincerely,

Kearney & Company

Kearney & Company, P.C.
August 11, 2016

BACKGROUND

Overview

On July 30, 2008, FHFA was established by the Housing and Economic Recovery Act of 2008 (HERA), Public Law (P.L.) No. 110-289. HERA abolished two existing Federal agencies, the Office of Federal Housing Enterprise Oversight (OFHEO) and the Federal Housing Finance Board (FHFB), and created FHFA to regulate the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), the 11 Federal Home Loan Banks (FHLBanks), and the FHLBanks Office of Finance.

FHFA is an independent Federal agency with a Director appointed by the President and confirmed by the United States (U.S.) Senate. The Agency's mission is to provide effective supervision, regulation, and housing mission oversight of Fannie Mae, Freddie Mac, and the 11 FHLBanks, in addition to the FHLBanks Office of Finance. FHFA is a non-appropriated, non-apportioned agency that draws its financial resources from assessments on Fannie Mae, Freddie Mac, and the 11 FHLBanks.

In June 2015, the Office of Personnel Management (OPM) announced that hackers had exploited inadequate controls to gain system access and steal Social Security Numbers (SSN) and other personal information in background investigation files. Following the data breach at OPM, the Office of Management and Budget (OMB) directed Federal agencies to immediately take corrective actions. In light of this breach and other attacks targeting government systems, there is an increased need for protection of sensitive Federal data.

Cybersecurity Act of 2015

The Cybersecurity Act of 2015, included as Division N of the 2016 Consolidated Appropriations Act, directs Inspectors General of agencies operating Federal computer systems that provide access to PII, to submit a report to the U.S. Congress, which shall include the following information collected from the agency:

1. A description of the logical access policies and practices used to access a PII system, including whether appropriate standards were followed
2. A description and list of the logical access controls and multi-factor authentication used by the agency to govern access to PII systems by privileged users
3. A description of policies and procedures followed to detect data exfiltration and maintain an inventory software and licenses on the covered systems
4. A description of policies and procedures to ensure that contractors and other entities providing services to the agency implement appropriate data security management practices.

NIST Security Standards and Guidelines

NIST provides standards and guidelines pertaining to Federal information systems. The standards prescribe information security requirements necessary to improve the security, privacy, and overall protection of Federal information and information systems. Federal agencies must comply with NIST's Federal Information Processing Standards (FIPS) and Special Publications (SP) as recommended guidance documents.

Results of Audit

Kearney found that FHFA has satisfied required security and privacy controls for the six sampled covered systems. In addition, FHFA has implemented controls to protect against cyber-attacks originating from foreign countries.

1. Logical Access Policies and Practices for Covered Systems

To properly manage the identification and authentication of authorized users, an organization's first step is to document and implement the logical access policies and practices that form the basis of how users will connect to the organization's network and internal and external systems. Logical access is wide-ranging and requires organizations to consider such topics as enforcement of secure passwords, uniquely identifying users, and providing users with only the access needed to complete job responsibilities. FHFA has documented and implemented such logical access policies and procedures. Specifically, our audit confirmed the following:

- Account Provisioning Controls:
  - System managers and security personnel create and configure network and system accounts to uniquely identify user accounts, only allowing access to data to perform applicable job functions. Roles are implemented to prevent general users from accessing administrative functions and system accounts are reviewed to identify inactive users.
- Password Complexity and Security:
  - FHFA system policy ensures passwords are sufficiently complex to prevent easy guessing. Complexity configurations include minimum length, as well as requirements for uppercase and lowercase letters, numerals, and special characters.
  - When authenticating to the system, FHFA systems obscure authenticators (whether passwords or personal identification number [PIN] codes) to prevent an unauthorized party from viewing the password when entered.
- Functional Responsibilities
  - FHFA has documented the Agency roles responsible for ensuring that controls are in place and operating effectively. This includes FHFA system owners performing reviews of user authorizations and privilege levels, as well as managers following FHFA procedures for obtaining and removing access to information resources for assigned staff.

For information systems hosted by other organizations, FHFA's information security staff reviews the external system's security assessment and authorization (SA&A) packages prior to authorizing FHFA use to ensure that they meet the minimum requirements of the FHFA SA&A

process. Through this review, they confirm that the external system complies with FHFA's requirements for logical access.

2. Logical and Multi-Factor Access to Covered Systems for Privileged Users

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: 1) something you know (e.g., password, PIN); 2) something you have (e.g., cryptographic identification device, token); or 3) something you are (e.g., biometric). Implementing multi-factor authentication controls for users with elevated access to sensitive data reduces risk that an attack using a compromised user ID and password would be successful. Kearney observed users log into six covered systems and documented the technologies implemented to authenticate privileged and traditional end-users.

System	Authentication Method	Additional Details
Correspondence Tracking System (CTS)	[redacted]	CTS is only accessible through the FHFA network, which requires two-factor authentication upon desktop start.
FOIAXpress	[redacted]	The system is custom software designed for Federal use, but the system vendors has not implemented [redacted] authentication capability. As a compensating control, the system is only accessible by users on the FHFA network, which requires two-factor authentication upon desktop start.
Merit Central/Job Performance Plan (JPP)	[redacted]	Users access the system via web browser and authentication occurs in the background without the need for entering a separate user ID and password (e.g., single sign-on).
FHR Navigator	[redacted]	A one-time passcode is sent via text message to users accessing via user ID and password.
iComplaints:	[redacted]	This is a Commercial Off-the-Shelf (COTS) product that has not [redacted] for privileged and general users.
EmployeeExpress (EEX)	[redacted]	FHFA users do not have privileged accounts on EEX. FHFA management noted that OPM has implemented two-factor authentication for internal users that administer the system and plans to expand two-factor

System	Authentication Method	Additional Details
		authentication to external users at a future date.
Administrative Access to FHFA servers hosting covered systems	[redacted]	Administrator accounts are tied to [redacted] authentication.

3. Software Licensing and Installed Software on Covered Systems

It is important that organizations have the ability to document the current state of the software installed, authorized, and used on devices that access systems and data. A current and comprehensive software inventory assists with ensuring organizations know which patches and software updates are needed to minimize software vulnerabilities, as well as what software configurations are necessary to comply with established configuration baselines.

FHFA demonstrated its ability to monitor and perform a software inventory on the sampled covered systems and confirm that all software licenses for the internal systems reviewed (CTS, Merit Central/JPP, and FOIAXpress) were properly licensed. Specifically, FHFA's System Security Plan (SSP) included the servers, hardware components, operating system (OS) and version, database and version, and installed software and version information. The Audit Team observed information technology (IT) management review the installed software on the servers maintaining the source code libraries for the systems and compared this information to the respective SSPs, without exception.

The inventory of software installed on two internal servers hosting three applications was consistent with their SSPs. Regarding installation of security patches for deployed software, FHFA's Vulnerability Assessment process includes a weekly scan of servers and desktops and identifies servers and desktops that are not fully patched. FHFA has documented procedures for tracking software licenses and ensuring that non-approved software installed on systems is removed. FHFA's system administrators use Microsoft licensing tools to automate the monitoring of versions and planning for future needs based on expected usage. During our audit, system administrators demonstrated the process for ensuring that Microsoft OS, virtual servers, and user software are current and supported by the vendor.

4. Security Management Practices Used to Monitor and Detect Data Exfiltration

The CSA identifies the following technical solutions **(in bold)** that assist in preventing unauthorized transfer of sensitive data outside of organizational control:

- **Data Loss Prevention (DLP) technologies -** DLP technologies are generally content-aware solutions that can monitor for sensitive data (e.g., SSN, bank account numbers, etc.) in motion by inspecting network communications, such as e-mail, Instant Messaging, web, file transfers, and peer-to-peer communication. Automated systems can block the information transfer if it violates a data security policy or by encrypting the data for secure exchange while not interfering with legitimate business.

- **Forensic technologies -** Forensic technologies are used to gather evidence of an incident through the identification, collection, examination, and analysis of data, while preserving the integrity of the information and maintaining a strict chain of custody for the data.
- **Digital Rights Management (DRM) technologies -** DRM technologies are implemented to manage the trusted distribution and control of protected content to users and devices authorized by an organization. Typical DRM solutions include a combination of technologies (e.g., encryption, digital watermarking) and policies (e.g., location restrictions, authorized access times).

Addressed as part of the entity-wide controls, FHFA has documented and implemented specific data exfiltration prevention capabilities, including DLP and forensic technology to provide visibility over sensitive data traversing its network. The FHFA General Support System (GSS) Information Security Architecture document notes the implementation of a secured email solution to protect sensitive data from being sent outside the agency unencrypted. The FHFA GSS SSP notes that systems and audit log applications are configured to produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

	DLP	Forensics and Visibility	DRM
FHFA Implementation	FHFA's secure email solution automatically encrypts e-mails from leaving FHFA network with PII.	FHFA relies on firewall/ Intrusion Prevention System (IPS) logs and third-party forensic case management software for network and endpoint forensic investigation, respectively.	FHFA has not implemented DRM capabilities.
Additional Details	The solution automatically recognizes plaintext communicated in the body of the message and/or in attachments that meet predefined policies, including SSN, financial identifiers and health care identifiers.	FHFA implemented audit monitoring controls on the FHFA GSS based on NIST SP 800-53, Audit and Accountability control family.	FHFA noted that DRM is not required by NIST SP 800-53 for moderate impact systems. Further, FHFA stated the resources required to implement, manage, and maintain a DRM solution exceeded expected benefits.

5. Oversight of Contractor Implementation of Software Management and Data Exfiltration Controls

Agencies benefit from the economies of scale in reusing Government-ready platforms that provide similar services across multiple agencies. With the potential benefits, agencies must establish processes to ensure adequate security of the external entities and their information system. In this regard, we determined that FHFA periodically performs a review of the SA&A documents made available through the Federal Risk and Authorization Management Program (FedRAMP) or from the external system management. FHFA IT personnel can examine the external systems' SSP and confirm the implementation of specific security controls, such as DLP, forensics capability, and software and license management. Reviewing the Security Assessment Reports (SAR) and resulting Plans of Action and Milestones (POA&M), FHFA can confirm the operating effectiveness of specific security controls. For each external system, FHFA reviews and concludes on compliance with FHFA's requirements and the external systems' suitability to host FHFA data prior to use by FHFA. FHFA does not require its external systems to implement DLP, forensic technologies, or DRM, as these controls are not required by NIST SP 800-53 or added to a system's moderate security baseline.

Compensating Security Controls

FHFA management stated that while they have not implemented DRM technologies, they have taken other steps to prevent the loss of sensitive information, such as PII. These additional security measures include encrypting specific PII data fields at rest in FHFA databases [redacted]. FHFA's firewall also blocks unsolicited inbound packets from a number of nations outside of the United States and plans to expand this filtering control to block all inbound and outbound traffic to non-U.S. Internet Protocol (IP) addresses. FHFA mobile devices utilize full disk encryption and Universal Serial Bus (USB) ports are restricted to prevent the export of FHFA data to external storage devices.

Summary of FHFA's CSA Control Implementations

FHFA has implemented security and privacy policies, procedures, and supporting technology to protect PII. Below is a summary of key practices requested by the CSA.

1. **Logical Access Policies and Practices for Covered Systems**
   FHFA has documented and implemented logical access policies and practices that were consistent with OMB policy and applicable NIST guidelines for the six selected systems.
2. **Logical and Multi-Factor Access to Covered Systems for Privileged Users**
   FHFA has employed logical access controls for covered systems consistent with policies and procedures and requires system administrators to use multi-factor authentication to access internal system resources.
3. **Software Licensing and Installed Software on Covered Systems**
   FHFA manages installed software for covered systems and ensures that software is properly licensed. FHFA has an automated means to monitor and track versions and licenses used. All server software is current and supported by the vendor.
4. **Security Practices Used to Monitor and Detect Data Exfiltration**
   FHFA has automated means to encrypt and securely deliver e-mail containing PII and financial information. FHFA relies on firewall logs and forensic case management

software for network and endpoint forensic investigation, respectively. Network devices, such as servers and routers, transmit their security logs to a centralized audit logging solution to facilitate audit log analysis and comply with specific NIST SP 800-53 auditing controls. FHFA management has not implemented DRM solutions as they are not a requirement for moderate-risk, non-national security systems.

5. **Oversight of Contractor Implementation of Software Management and Data Exfiltration Controls**
   FHFA reviews the security assessments and authorization documents of externally hosted systems and services. It is important to note that while a review of an external systems' SSP and POA&Ms would identify issues with audit monitoring and software inventory and license management, this review does not include assessments of data loss prevention, forensic technologies, or DRM capabilities (unless specifically detailed), as these controls are not required in a system's "moderate" baseline under NIST SP 800-53 Rev. 4 controls.
6. **CSA-Related Privacy Program Controls**
   To verify that PII is being managed and protected in compliance with Federal requirements, Kearney interviewed FHFA privacy officials and reviewed documentation of FHFA's Privacy Program for controls related to the CSA's focus areas. On a sample basis, we confirmed that FHFA has implemented required privacy controls found in NIST SP 800-53, Appendix J: *Privacy Control Catalog*. Please refer to **Appendix A** for complete details of tested controls.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this performance audit was to report information to the U.S. Congress detailing the Federal Housing Finance Agency's (FHFA) establishment and implementation of logical access, software management, and data exfiltration controls on covered systems. Kearney & Company, P.C.'s (Kearney) methodology for this audit included an assessment of six FHFA information systems for compliance with selected controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, found in Appendix J: *Privacy Control Catalog*.

Kearney conducted our performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion. Our CSA approach, which is based on NIST SP 800-53, Rev. 4 and the CSA, employed the interview and inspection assessment methods.

Kearney's audit program included procedures to test and report on: 1) five Section 406 requirements, as identified in the CSA, and 2) a selection of NIST SP 800-53, Rev. 4 privacy controls. See ***Table 1*** and ***Table 2***.

Table 1: CSA, Section 406 Requirements

APG #	Section 406 Requirements
1.0	Description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
2.0	Description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
3.0	Description of the reasons for not using logical access controls or multi-factor authentication (if not used for connecting to a covered system).
4.1	Description of policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
4.2	Description of what capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including: a. Data Loss Prevention (DLP) capabilities b. Forensics and visibility capabilities c. Digital Rights Management (DRM) capabilities.
4.3	Description of how the covered agency is using the data exfiltration capabilities in clause 4.2.

APG #	Section 406 Requirements
4.4	If the covered agency is not utilizing data exfiltration (i.e., prevention) capabilities described in clause 4.2, a description of the reasons for not utilizing such capabilities.
5.0	Description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in parts 4.1-4.4 above.

Table 2: NIST SP 800-53, Rev. 4, Appendix J: Privacy Controls

Control # and Name	Privacy Control
AR-1 Governance and Privacy Program	The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems. b. Monitors Federal privacy laws and policy for changes that affect the privacy program. c. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program. d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures. e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. f. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].
AR-2 Privacy Impact and Risk Assessment	The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII b. Conducts Privacy Impact Assessments (PIA) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
AR-3 Privacy Requirements for Contractors and Service Providers	The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers b. Includes privacy requirements in contracts and other acquisition-related documents.

Control # and Name	Privacy Control
AR-4 Privacy Monitoring and Auditing	The organization: a. Implements a method to audit privacy controls on a regular basis b. Implements a process to embed privacy considerations into the life cycle of PII, programs, and systems c. Monitor systems that maintain PII d. Ensure access to PII is limited to privileged users
AR-5 Privacy Awareness and Training	The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII [Assignment: organization-defined frequency, at least annually] c. Ensures that personnel certify, manually or electronically, acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].
SE-1 Inventory of Personally Identifiable Information	The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII b. Provides each update of the PII inventory to the Chief Information Officer (CIO) or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.
SE-2 Privacy Incident Response	The organization: a. Develops and implements a Privacy Incident Response Plan b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Control # and Name	Privacy Control
TR-2 System of Records Notices and Privacy Act Statements	The organization: a. Publishes System of Records Notices (SORN) in the Federal Register, subject to required oversight processes, for systems containing PII b. Keeps SORNs current c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Kearney's overarching rationale and approach to the system selection process was to select systems for testing that would address requirements identified in the CSA. Based on our review of prior-year Federal Information System Modernization Act of 2014 (FISMA)[3] audit documentation and analysis of FHFA's system inventory documentation, we selected a sample of information systems using the following criteria:

- Systems that contain sensitive PII data
- Systems with moderate impact FIPS 199 categorization
- An even distribution of internal and external PII systems
- Sample size is a selection of 25% of the total number of PII systems.

Based on these criteria, Kearney selected six systems for testing, as listed in ***Table 3***.

Table 3: FHFA Systems Selected for Assessment

Covered System Name	Description	FIPS PUB 199 Categorization	Owner
Correspondence Tracking System (CTS)	The purpose of the system is to capture and track correspondence that FHFA receives from external sources. The system captures information on the sender and the nature of the correspondence (e.g., name; property, home, and business address; e-mail address; telephone numbers; and other personal and contact information). The system helps ensure that FHFA responds to the inquiry in a timely and accurate manner.	Moderate	FHFA
FOIAXpress	The purpose of the system is to assist FHFA in receiving, processing, and tracking Freedom of Information Act (FOIA) and Privacy Act requests from the public.	Moderate	FHFA
Merit Central/ Job	The system is an automated tool that facilitates the annual FHFA-wide merit increase and Performance-Based Bonus (PBB) decision-	Moderate	FHFA

[3] Kearney performed the prior year (2015) FISMA audit of FHFA under contract with FHFA OIG.

Covered System Name	Description	FIPS PUB 199 Categorization	Owner
Performance Plan (JPP)	making and processing, as well as to conduct salary planning determinations. The system is an internal system developed in close conjunction between the Office of Human Resources Management (OHRM) and the Office of Technology and Information Management (OTIM).		
Employee Express (EEX)	The purpose of the automated system is to enable employees to manage their own discretionary payroll and personnel transactions.	Moderate	External
Federal Human Resources (FHR) Navigator	The purpose of the system is to automate Federal human resources functions within a single platform. It is a suite of web-based software tools that is supported by a centralized database to facilitate the strategic management of human capital within the Federal workplace.	Moderate	External
MicroPact iComplaints	The system is used to track, manage, and report on Equal Employment Opportunity (EEO) complaints. Information collected is kept confidential for use during the alternate dispute resolution process. Additionally, data is used to create statistical reports.	Moderate	External

Kearney performed fieldwork for the FHFA CSA audit from May to July of 2016. Throughout the CSA audit, we met with FHFA management to discuss preliminary observations. Kearney's work in support of the audit was guided by applicable FHFA policies and Federal criteria, including the following:

1. Privacy Act of 1974, 5 United States Code (U.S.C.) § 552
2. FISMA
3. E-Government Act of 2002 (Public Law [P.L.] 107-347)
4. Section 406, CSA
5. Federal Acquisition Regulation (FAR), 48 C.F.R. Part 24
6. OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*
7. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
8. OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*
9. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
10. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
11. OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*

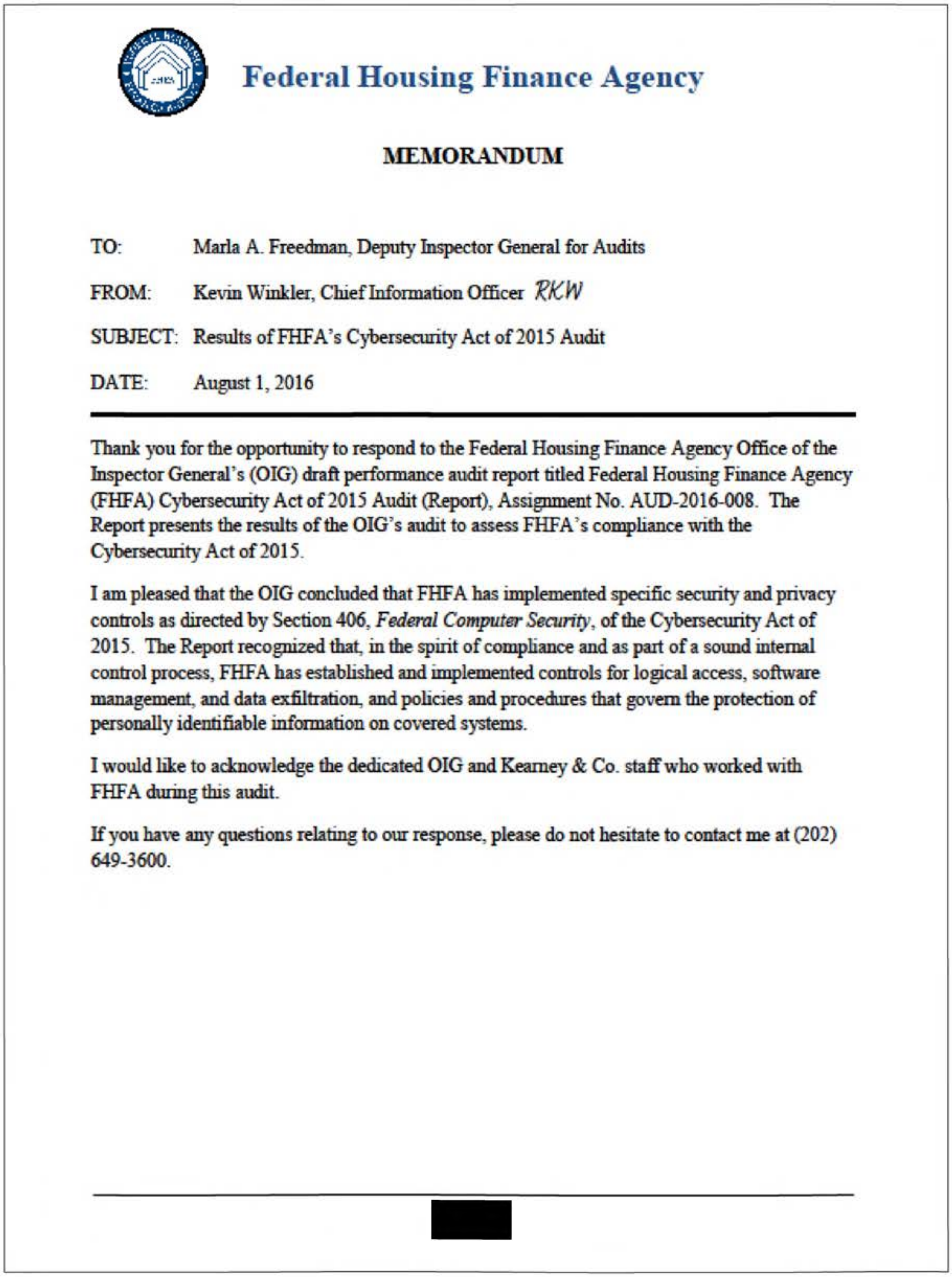
12. OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*
13. NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems; A Security Life Cycle Approach*
14. NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
15. NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J: *Privacy Control Catalog*
16. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
17. Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
18. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems.*
19. FHFA, *General Support Systems (GSS) Information Security Architecture*
20. FHFA, *Security Awareness and Training Procedures*
21. FHFA, *Information Security Incident Response Plan*
22. FHFA, *Procedures for Monitoring of Information Technology Systems that Contain Personally Identifiable Information*
23. FHFA, *Security Assessment and Authorization Procedure*
24. FHFA, *Identification and Authentication Standard*
25. FHFA, *Access Control Standard*
26. FHFA, *Privacy Program Plan*

APPENDIX B: ASSESSMENT MATRIX

The purpose of the matrix below is to identify the Cybersecurity Act of 2015 (CSA) questions and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, Appendix J security control(s) and detail if the testing performed touched on general controls or applications selected for assessment.

CSA/NIST Questions	General Control	Application Controls	
	GSS	FHFA Internal Systems (CTS, FOIAXpress, Merit Central/JPP)	External Systems (EEX, FHR Navigator, iComplaints)
1. CSA, Section 406: Logical Access Policy and Practices	X	X	X
2. CSA, Section 406: Logical Access Multi-Factor Authentication	X	X	X
3. CSA, Section 406: Software and License Inventories	X	X	Not Applicable (N/A)
4. CSA, Section 406: Data Exfiltration	X	N/A	N/A
5. CSA, Section 406: 3rd Party Information Security Oversight	X	N/A	X
6. Governance and Privacy Program	X	N/A	N/A
7. Privacy Impact and Risk Assessment	X	X	X
8. Contractor Privacy Requirements	X	N/A	X
9. Monitoring/ Auditing	X	X	N/A
10. Training	X	N/A	N/A
11. System Inventory	X	X	X
12. Incident Response	X	X	X
13. SORNs/Privacy Act Statements	X	X	X

APPENDIX C: FHFA's MANAGEMENT RESPONSE



Federal Housing Finance Agency

MEMORANDUM

TO: Marla A. Freedman, Deputy Inspector General for Audits

FROM: Kevin Winkler, Chief Information Officer RKW

SUBJECT: Results of FHFA's Cybersecurity Act of 2015 Audit

DATE: August 1, 2016

Thank you for the opportunity to respond to the Federal Housing Finance Agency Office of the Inspector General's (OIG) draft performance audit report titled Federal Housing Finance Agency (FHFA) Cybersecurity Act of 2015 Audit (Report), Assignment No. AUD-2016-008. The Report presents the results of the OIG's audit to assess FHFA's compliance with the Cybersecurity Act of 2015.

I am pleased that the OIG concluded that FHFA has implemented specific security and privacy controls as directed by Section 406, *Federal Computer Security*, of the Cybersecurity Act of 2015. The Report recognized that, in the spirit of compliance and as part of a sound internal control process, FHFA has established and implemented controls for logical access, software management, and data exfiltration, and policies and procedures that govern the protection of personally identifiable information on covered systems.

I would like to acknowledge the dedicated OIG and Kearney & Co. staff who worked with FHFA during this audit.

If you have any questions relating to our response, please do not hesitate to contact me at (202) 649-3600.

[redacted]

ADDITIONAL INFORMATION AND COPIES

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219