FEDERAL HOUSING FINANCE AGENCY
OFFICE OF INSPECTOR GENERAL

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Information Security Program - 2011

Audit Report: AUD-2011-002 **Dated: September 29, 2011**

FEDERAL HOUSING FINANCE AGENCY
OFFICE OF INSPECTOR GENERAL
AT A GLANCE

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Information Security Program - 2011

Why FHFA-OIG Contracted for Audit

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agency-wide information security programs to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA requires agencies to undergo an annual independent evaluation of their information security programs and practices and an assessment of compliance with FISMA. Moreover, FISMA requires the National Institute of Standards and Technology (NIST) to issue standards and guidelines for Federal information and systems including minimum security requirements. NIST has defined an overall information security risk management framework.

Additionally, the Office of Management and Budget (OMB) has issued guidance related to information security including plans of action and milestones (POA&Ms) for addressing findings from security control assessments, security impact analyses, and continuous monitoring activities. POA&Ms provide a roadmap for continuous agency security improvement and assist agency officials to prioritize corrective action and resource allocation.

The Federal Housing Finance Agency (FHFA) Office of Inspector General (FHFA-OIG) contracted with Clifton Gunderson LLP (CG) to conduct a performance audit to fulfill its FISMA responsibilities for an annual independent evaluation of FHFA's security program. The objective of the audit was to evaluate the effectiveness of FHFA's information security program and practices and its compliance with FISMA and related information security policies, procedures, standards, and guidelines.

What FHFA-OIG Recommends

FHFA-OIG adopted CG's findings and recommendations. The audit report makes five recommendations to FHFA to strengthen its information security program: (1) finalize the agency-wide information security program plan; (2) update policies and procedures to address all NIST requirements and recommendations applicable to the FHFA information security environment; (3) develop and implement an information categorization policy and methodology; (4) establish a process to monitor compliance with procedures for timely completion of POA&Ms; and (5) track and monitor remediation actions to address weaknesses identified in network vulnerability assessments.

In response to the findings and recommendations, FHFA provided written comments, dated September 19, 2011. The Agency agreed with the recommendations. The complete text of the written comments can be found in Appendix B of this report.

What Clifton Gunderson LLP Found (See Appendix A of this Report)

FHFA generally has a sound risk management framework for its information security program. However, information security practices were not fully effective to preserve the confidentiality, integrity, and availability of FHFA's information and information systems, potentially exposing FHFA's information resources to unauthorized access, use, disclosure, disruption, modification, or destruction.

Although FHFA's information security program had a number of strengths, including but not limited to its information system security training, system-level planning, risk assessment, access authorization, and continuous control monitoring, the audit identified security practices that can be improved. Specifically, FHFA had not:

- Finalized, disseminated, and implemented a NIST-recommended organization-wide information security program plan that defines such key requirements as security-related roles and responsibilities and security program controls.
- Updated the Agency's policies and procedures to address completely all of the NIST-recommended components within the control families applicable to the FHFA information system environment. For example, key controls in areas such as access control, configuration management, contingency planning, and incident handling were not fully addressed by FHFA.
- Developed, disseminated, and implemented an agency-wide information categorization policy and methodology. FHFA had categorized its information systems without categorizing the information used by those systems. NIST describes controls related to security categorization, which provides a basis for selecting and implementing controls.
- Implemented adequate procedures for tracking and monitoring correction of weaknesses or deficiencies through POA&Ms. As defined by NIST, the plans should identify tasks needing to be accomplished, resource requirements, milestones for meeting tasks, and completion dates for milestones.
- Implemented adequate procedures for ensuring remediation of weaknesses noted in network vulnerability assessments. Numerous vulnerabilities identified during these assessments were not tracked and monitored to completion.

Addressing these control deficiencies in information security practices will strengthen FHFA's information security program and contribute to ongoing efforts to achieve reasonable assurance of adequate security over information resources.

TABLE OF CONTENTS

ABBREVIATIONS

CG ..... Clifton Gunderson
C&A ..... Certification and Accreditation
CIO ..... Chief Information Officer
CISO ..... Chief Information Security Officer
Fannie Mae ..... Federal National Mortgage Association
FHFA ..... Federal Housing Finance Agency
FHFA-OIG ..... Federal Housing Finance Agency Office of Inspector General
FHLBanks ..... Federal Home Loan Banks
Freddie Mac ..... Federal Home Loan Mortgage Corporation
FIPS ..... Federal Information Processing Standards
FISMA ..... Federal Information Security Management Act of 2002
GSS ..... General Support System
GAGAS ..... Generally Accepted Government Auditing Standards
HERA ..... Housing and Economic Recovery Act of 2008
IT ..... Information Technology
NIST ..... National Institute of Standards and Technology
OMB ..... Office of Management and Budget
POA&M ..... Plan of Action and Milestones
RMF ..... Risk Management Framework

Federal Housing Finance Agency

Office of Inspector General

Washington, DC

PREFACE

FHFA-OIG was established by the Housing and Economic Recovery Act of 2008 (HERA),[1] which amended the Inspector General Act of 1978.[2] FHFA-OIG is authorized to conduct audits, investigations, and other activities of the programs and operations of FHFA; to recommend policies that promote economy and efficiency in the administration of such programs and operations; and to prevent and detect fraud and abuse in them. This is one in a series of audits, evaluations, and special reports published as part of FHFA-OIG's oversight responsibilities to promote economy, effectiveness, and efficiency in the administration of FHFA's programs.

The objective of this performance audit was to evaluate FHFA's information security program and practices, including FHFA's compliance with the FISMA and related information security policies, procedures, standards, and guidelines. FHFA-OIG contracted with CG to conduct this statutorily required audit. CG's audit report is included in Appendix A of this report.

CG's audit report makes five recommendations to FHFA to assist in strengthening its information security program. FHFA-OIG adopts these recommendations and believes they will help the Agency achieve more economical, effective, and efficient operations. FHFA-OIG appreciates the assistance of all those who contributed to the audit.

This report has been distributed to Congress, OMB, and others and will be posted on FHFA-OIG's website, www.fhfaoig.gov/.

Russell A. Rau
Deputy Inspector General for Audits

[1] Public Law No. 110-289.

[2] Public Law No. 95-452.

APPENDIX A

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Information Security Program – 2011, pages 1 – 38.

COUNT ON INSIGHT®

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Clifton Gunderson LLP's Independent Audit of the Federal Housing Finance Agency's Information Security Program - 2011

Prepared for the
Federal Housing Finance Agency
Office of Inspector General

September 29, 2011

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552

www.cliftoncpa.com

Table of Contents

Executive Summary

September 29, 2011

Honorable Steve A. Linick
Inspector General
Federal Housing Finance Agency
1625 Eye Street, NW
Washington, DC 20006

Dear Mr. Linick:

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA requires agencies to undergo an annual independent evaluation of the agency's information security programs and practices and an assessment of compliance with the requirements of the Act. The Federal Housing Finance Agency (FHFA) Office of Inspector General (FHFA-OIG) contracted with Clifton Gunderson (CG) to conduct a performance audit of the FHFA's information security program and practices related to FISMA. We are pleased to provide the Fiscal Year (FY) 2011 FISMA CG Independent Audit Report, detailing the results of our review of FHFA's information security program.

The objective of this performance audit was to evaluate the effectiveness of FHFA's information security program and practices, including FHFA's compliance with FISMA and related information security policies, procedures, standards and guidelines. The FHFA-OIG's approach for the FY 2011 FISMA audit was a programmatic review of FHFA's governance structure related to the implementation and monitoring of FISMA requirements, and how FHFA has applied the National Institute of Standards and Technology's (NIST's) Risk Management Framework (RMF) for managing security throughout the lifecycle of their information systems. The audit included a review of the FHFA's Office of the Chief Information Officer's (CIO's) oversight role related to the implementation and monitoring of FISMA requirements, as well as the review of a selection of security controls within each of the RMF phases for a sample of information systems, as required by FISMA. The controls assessed include the following NIST Special Publication (SP) 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST SP 800-53 Rev.3), control families: Planning (PL), Risk Assessment (RA) and Security Assessment and Authorization (CA). Our audit was performed in accordance with *Generally Accepted Government Auditing Standards* (GAGAS).

We found that FHFA generally has a sound RMF for its information security program. In particular, strengths of the program included training, system-level security planning, risk assessment, authorization of system connectivity, and continuous monitoring of

security controls. However, information security practices were not fully effective to preserve the confidentiality, integrity and availability of FHFA's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. CG does not consider the deficiencies noted as a significant deficiency under FISMA.[1] However, CG concluded collectively that the deficiencies are significant in the context of the audit objective as defined for performance audits under GAGAS.

For example, the audit identified a number of FHFA's security practices that can be improved. Specifically, FHFA had not:

- Finalized, disseminated, and implemented an organization-wide information security program plan.
- Updated the Agency's information system policies and procedures to completely address all of the components within the control families from NIST SP 800-53 Rev. 3 applicable to the FHFA information system environment.
- Developed, disseminated, and implemented an agency-wide information categorization policy and methodology.
- Implemented adequate procedures for tracking and monitoring weaknesses or deficiencies through Plan of Action and Milestones (POA&M).
- Implemented adequate procedures for tracking and monitoring remediation of weaknesses noted from network vulnerability scans.

Addressing these control deficiencies in information security practices will strengthen FHFA's information security program and contribute to ongoing efforts to achieve reasonable assurance of adequate security over information resources.

FHFA's information security program also had a number of strengths, including but not limited to the following:

- Providing initial security awareness training to new employees and annual refresher training as well as security specific role based training for FHFA security staff.
- Developing security plans for individual information systems that describe the security controls in place or planned for meeting security requirements and assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Conducting an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or

[1] See page 33 in this report for the definition of significant deficiency under FISMA.

destruction of the information system and the information it processes, stores or transmits, and documenting risk assessment results in a risk assessment report.

— Authorizing connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements.

— Establishing a continuous monitoring strategy and implementing a continuous monitoring program that includes ongoing security control assessments and reporting the security state of the information system to appropriate organizational officials.

This report makes five recommendations to assist FHFA in strengthening its information security program.

This performance audit did not constitute an audit of financial statements in accordance with GAGAS. CG was not engaged to, and did not, render an opinion on the FHFA's internal controls over financial reporting or financial management systems. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that controls may become inadequate because of changes in conditions, or because compliance with controls may deteriorate.

Sincerely,

CLIFTON GUNDERSON LLP

Clifton Gunderson LLP

Arlington, Virginia
September 29, 2011

Background

On July 30, 2008, FHFA was established by the Housing and Economic and Recovery Act of 2008 (HERA), Public Law No. 110-289. Specifically, HERA abolished two existing Federal agencies, the Office of Federal Housing Enterprise Oversight and the Federal Housing Finance Board, and in their place created the FHFA to regulate the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), the 12 Federal Home Loan Banks (FHLBanks), and the Office of Finance. FHFA is an independent Federal agency, with a Director, appointed by the President and confirmed by the U.S. Senate. Its mission is to provide effective supervision, regulation, and housing mission oversight of Fannie Mae, Freddie Mac and the FHLBanks. FHFA is a non-appropriated, non-apportioned agency that draws its financial resources from assessments on Fannie Mae, Freddie Mac, and the 12 FHLBanks. The Agency has a $201 million budget for fiscal year 2011 and a staff of 598.[2]

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 (FISMA) was enacted into law as Title III of the E-Government Act of 2002 (Public Law No. 107-347, December 17, 2002). Key requirements of FISMA include:

- The establishment of an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
- An annual independent evaluation of the agency's information security programs and practices; and
- An assessment of compliance with the requirements of the Act.

In addition, FISMA requires Federal agencies to implement the following:

- Periodic risk assessments;
- Information security policies, procedures, standards, and guidelines;
- Delegation of authority to the CIO to ensure compliance with policy;
- Security awareness training programs;
- Periodic testing and evaluation of the effectiveness of security policies, procedures, and practices to be done no less than annually;
- Processes to manage remedial actions for addressing deficiencies;

[2] The Appendix, Other Independent Agencies, Budget of the United States Government, Fiscal Year 2012, http://www.whitehouse.gov/sites/default/files/omb/budget/fy2012/assets/oia.pdf, pp. 1239-1241.

- Procedures for detecting, reporting, and responding to security incidents;
- Plans to ensure continuity of operations; and
- Annual reporting on the adequacy and effectiveness of the information security program.

The Office of Management and Budget (OMB) is responsible for reporting to Congress a summary of the results of agency compliance with FISMA requirements. OMB's principal written statement of government policy regarding information security is OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (OMB Circular A-130, Appendix III), dated November 28, 2000, which establishes a minimum set of controls to be included in Federal automated information security programs. In particular, Appendix III of OMB Circular A-130 defines adequate security as security commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Additionally, OMB has issued guidance related to information security with regard to plans of action and milestones (POA&Ms) for addressing findings from security control assessments, security impact analyses, and continuous monitoring activities. Per OMB Memoranda M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, POA&Ms provide a roadmap for continuous agency security improvement and assist agency officials with prioritizing corrective action and resource allocation.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to Federal information systems. Standards prescribed are to include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of Federal information and information systems. FISMA requires that Federal agencies comply with Federal Information Processing Standards (FIPS) issued by NIST. In addition, NIST develops and issues Special Publications (SPs) as recommendations and guidance documents. FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200), mandates the use of NIST SP 800-53 Rev. 3. The purpose of NIST SP 800-53 Rev. 3 is to provide guidelines for selecting and specifying security controls for information systems supporting the agency to meet the requirements of FIPS PUB 200. The security controls described in NIST SP 800-53 Rev. 3 are organized into 18 families. Each security control family includes security controls associated with the security functionality of the family. In addition, there are three

general classes of security controls: management, operational, and technical.[3] The NIST SP 800-53 Rev. 3 security control families are as follows:

Table 1: Security Control Families

Security Control Family	Control Class
Access Control	Technical
Audit and Accountability	Technical
Identification and Authentication	Technical
System and Communications Protection	Technical
Security Assessment and Authorization	Management
Planning	Management
Risk Assessment	Management
System and Services Acquisition	Management
Program Management	Management
Awareness and Training	Operational
Configuration Management	Operational
Contingency Planning	Operational
Incident Response	Operational
Maintenance	Operational
Media Protection	Operational
Physical and Environmental Protection	Operational
Personnel Security	Operational
System and Information Integrity	Operational

[3] According to NIST SP 800-53 Rev. 3, management controls are the security controls for an information system that focus on the management of risk and the management of information system security. Operational controls are the security controls for an information system that are primarily implemented and executed by people (as opposed to systems). Technical controls are the security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

NIST Risk Management Framework

FISMA also requires NIST to develop standards and guidelines to be used by agencies to categorize all information and information systems collected or maintained by or on behalf of the agency in order to provide appropriate levels of information security according to a range of risk levels. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems,* establishes security categories for information and information systems based on the potential impact on the agency should certain events occur which threaten the information and information systems needed by the agency. FISMA defines three security objectives for information and information systems, which are also incorporated in the OMB Circular A-130, Appendix III, definition of adequate security:

Confidentiality – A loss of confidentiality is the unauthorized disclosure of information.

Integrity – A loss of integrity is the unauthorized modification or destruction of information.

Availability – A loss of availability is the disruption of access to or use of information or an information system.

To assist agencies in improving information security and strengthening risk management processes, NIST in partnership with the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems, developed a common information security framework, NIST's RMF. The RMF, comprised of the following six steps, provides a structured practice for incorporating information security and risk management activities into the system development life cycle:

- **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

- **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

- **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.

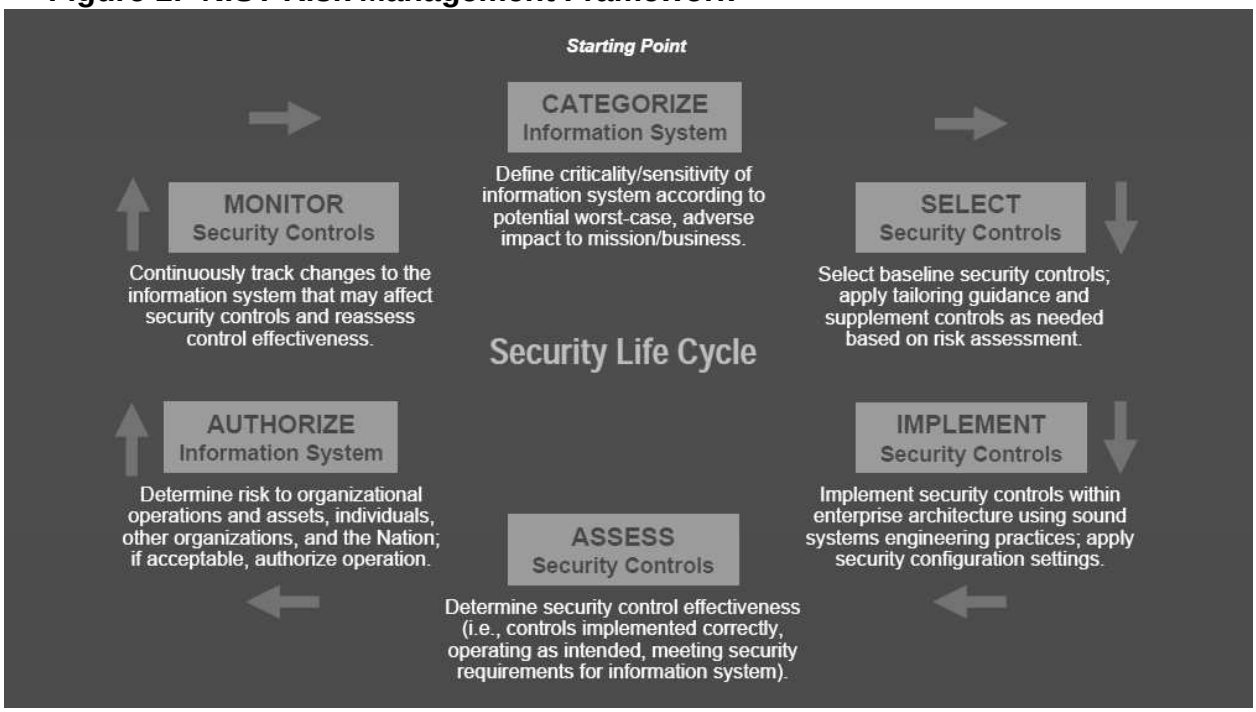
- **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

— **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

— **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST SP 800-37 Rev. 1), provides guidelines for applying the RMF to Federal information systems. This framework is detailed in the graphic below:

Figure 1: NIST Risk Management Framework



FHFA Systems Environment

FHFA defines the FHFA information system as a set of hardware, software, infrastructure and supporting personnel which work together to provide coordination, and decision making capabilities to the Agency. FHFA utilizes technology such as software, applications, and hardware for gathering, storing, processing, and transmitting information. All FHFA systems are identified as major or minor and categorized as high, medium, or low security impact based on FIPS PUB 199 standards. FHFA has one

General Support System (GSS),[4] 13 major applications, and 21 minor applications.[5] All of the systems are in the production phase of the life cycle except for one minor system in the development phase.

The major systems are:

Table 2: Major FHFA Systems

System	Life Cycle Status
CRS.Net – Call reporting system	Production
Examiner Workstation (xWorks)	Production
Avue System	Production
WebTA	Production
Information Management System (IMS)	Production
e-OPF	Production
FHR Navigator	Production
FMS – Financial Management System	Production
HSPD-12 PIV	Production
Managed Trusted Internet Protocol Service (MTIPS)	Production
National Finance Center (NFC)	Production
Plateau (LMS)	Production
USA Staffing	Production

FHFA defines boundaries for its information systems in order to assign protection resources to it. Agency information systems that are under the FHFA direct management control are called internal systems. FHFA defines externally hosted systems as contractor systems, which are not the Office of Technology and Information Management's (OTIM's) responsibility to operate and maintain. For externally hosted systems, Interagency Security Agreements are in place with other agencies. FHFA

[4] According to NIST SP 800-18 Rev. 1, *Guide to Developing Security Plans for Federal Information Systems,* a general support system is interconnected information resources under the same direct management control, which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

[5] According to NIST SP 800-37 Rev. 1, a major application is an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A minor application is an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

subsystems typically fall under the same management authority and are included within a single system security plan. These systems have the same function or mission objective and essentially the same operating characteristics and security needs, and reside in the same general operating environment. FHFA uses system boundaries for purposes of security accreditation.[6]

The FHFA GSS provides information sharing and data processing capabilities via interconnected workstations and servers. It is utilized by FHFA employees and contractors for network services, e-mail, and connectivity to FHFA's Intranet, local area network and the public Internet. FHFA employs a variety of applications (both commercial off-the-shelf products and custom applications developed in-house) running on the GSS. The GSS is extended for mobile device users using Exchange Server to support encrypted mobile devices. FHFA relies on the GSS automated information resources to accomplish its core business operations and processes. The FHFA GSS is a closed system, in that only FHFA-owned systems can directly connect to the network. It supports major and minor applications processing "sensitive but unclassified" information.

FHFA Information System Security Program

Organization

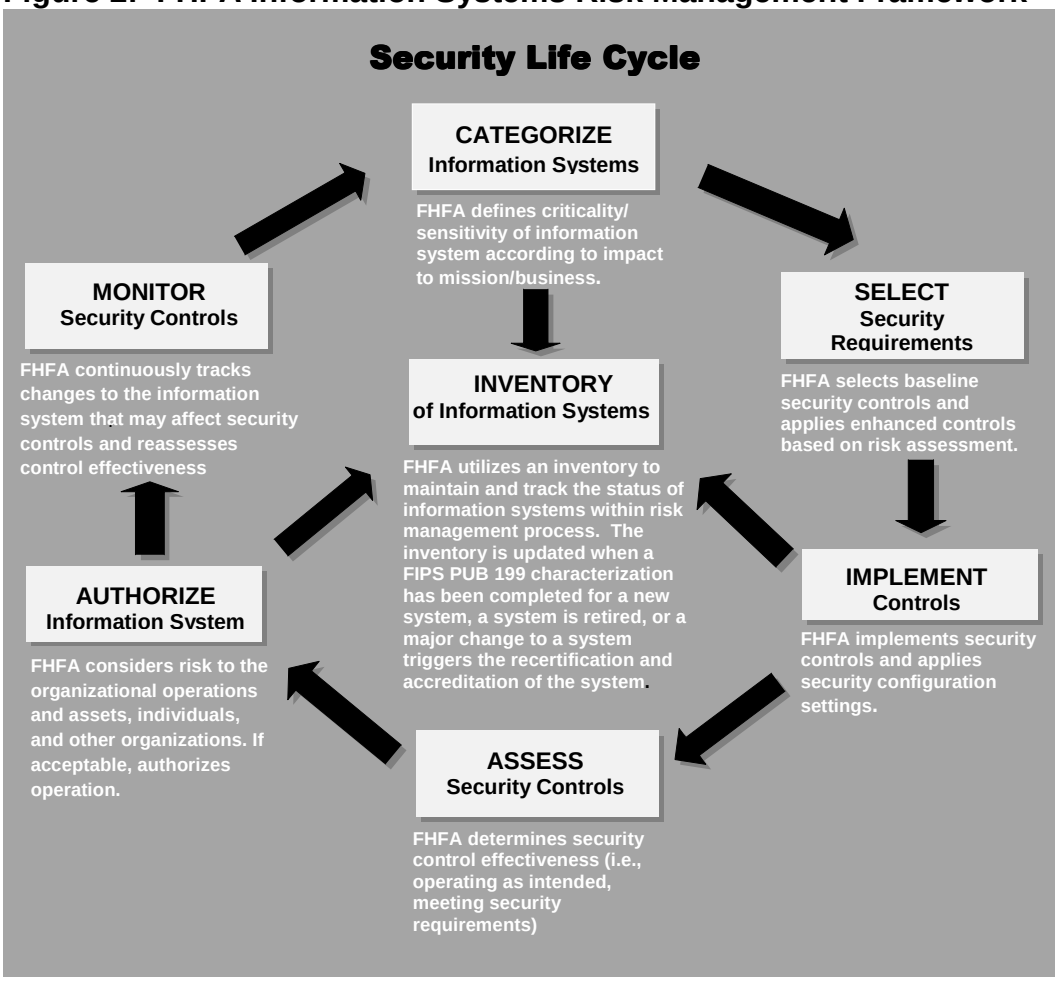
FHFA's information technology (IT) security organization includes the CIO, the Chief Information Security Officer (CISO), and eight additional staff responsible for training and awareness, network scanning and monitoring, and certification and accreditation (C&A) activities including continuous monitoring. The role of the CIO is to act as primary advisor to the Acting Director and senior FHFA staff on all matters related to information technology oversight, lead the analysis of technology requirements, and manage the life cycle of technology at FHFA. The CISO directs the management of FHFA's IT security program.

Risk Management

FHFA's information security program is based on NIST's RMF and provides FHFA the capability to manage information system-related security risks in line with the organization's mission and business objectives. Overall risk strategy for information systems is established by the senior leadership to ensure that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes. Following is a diagram depicting how FHFA is implementing NIST's RMF.

[6] According to NIST SP 800-53 Rev. 3, security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Figure 2: FHFA Information Systems Risk Management Framework



FHFA has developed an inventory of information systems that includes systems in production and development as part of its information systems risk management framework. The CISO reviews all new IT investments, which allow the OTIM security team to monitor the development of new systems and changes to existing systems. Systems must be approved by the CIO to be included in the inventory. The inventory is updated when a new system is approved, a system that is no longer used is retired, or a major change to a system triggers the security assessment and authorization of the system.

Information Security Policies and Procedures

FHFA has documented information security policies and procedures based on the controls defined by NIST SP 800-53 Rev. 3. The policies and procedures are organized by and cover each of the NIST SP 800-53 Rev. 3 control families. The information security policies and procedures are posted on the FHFA Intranet.

Security Awareness, Training, and Education

FHFA information system users are required to have annual security awareness training commensurate with their system responsibilities prior to gaining access to Agency information systems. Initial security awareness training is provided by requiring new system users to read and acknowledge FHFA's *Rules of Behavior*. Annual security awareness refresher training is provided using the Plateau Learning Management System, which tracks completion of training by all employees and contractors.

Incident Response

Network incidents are monitored by Managed Trusted Internet Provider. FHFA employees and contractors are required to immediately report all real or suspected computer security incidents to the FHFA Help Desk. The incident response team investigates incidents and reports the incidents to the CISO and CIO. Reporting of incidents to the United States Computer Emergency Readiness Team (US-CERT) is based on the category of the incident.[7]

Configuration Management

FHFA supports two distinct functions within configuration management. The first function, configuration management, determines the initial configuration of hardware and software. The other, change management, involves modifying hardware and software in production. FHFA's Change Control Board is responsible for the review and approval/rejection of all production change requests for updates to production environments. A Change Control Manager is responsible for ensuring system changes follow the change control process. The configuration management policy and procedures are used in conjunction with the system development life cycle methodology which establishes procedures, practices, and guidelines governing the system lifecycle of information systems within FHFA.

Contingency Planning

Information system owners are required to develop detailed business, communications, and IT recovery plans and the associated recovery capability for FHFA information systems. Recovery capability is tested annually. All personnel involved with the planning efforts are trained in executing the plan and the recovery capability is tested annually. In addition, a Continuity of Operations Program is developed including a Business Impact Analysis.

[7] According to NIST SP 800-53 Rev. 3, current Federal policy requires that all Federal agencies (unless specifically exempted from such requirements) report security incidents to the US-CERT within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

Security Performance Measurement

Security performance is measured by a monthly POA&M report,[8] which tracks open and closed POA&Ms. The security team discusses open POA&Ms with system owners each month and a quarterly meeting is held to discuss POA&M status. POA&M status for contractor systems is reviewed on a quarterly basis.

[8] According to NIST SP 800-53 Rev. 3, a POA&M is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Results of Audit

Overview

FISMA requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. Key elements of an organization-wide information security program include documentation of the information security program management controls that serve as the foundation for the agency's information security program, documentation of the security controls designated as common controls[9] and identifying the personnel within the agency responsible for the development, implementation, assessment, authorization, and monitoring of those controls. The organization-wide information security program plan combined with the security plans developed for each information system comprise the security controls employed by the agency in their entirety. A successful information security program is dependent upon the implementation of both the agency's program management controls as well as the implementation of the security controls for the agency's information systems.

The Agency's information system policies and procedures are critical in ensuring the organization-wide information security program is adhered to. The first security control in each NIST SP 800-53 Rev. 3 control family specifies the requirement for policies and procedures. These policies and procedures should provide clear guidance to Agency personnel as to what their responsibilities are with regard to information system security requirements.

CG's audit included performing a review of FHFA's governance structure related to the implementation of FHFA's information security program and a detailed review of the design for FHFA's information security policies and procedures to determine whether the policies and procedures, if properly implemented, would comply with NIST requirements for each security control family.

Additionally, CG assessed how FHFA has applied NIST's RMF for managing security of their information systems, which consists of six steps: 1 - Categorizing, 2 - Selecting, 3 - Implementing, 4 - Assessing, 5 - Authorizing, and 6 - Monitoring (as shown in Figure 1, page 10).

[9] According to NIST SP 800-53 Rev. 3, a common control is a security control that is inherited by one or more organizational information systems. Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

In order to evaluate how extensively FHFA has implemented the RMF, CG performed testing of selected NIST SP 800-53 Rev. 3 controls that correlate with each of the steps and tasks defined within the framework. Accordingly, CG tested program level controls including security categorization, information system inventory, risk assessment, security planning, security assessment, POA&Ms, and reviewed a judgmental sample of NIST SP 800-53 Rev. 3 controls related to information security program management.

We found that FHFA generally has a sound RMF for its information security program. In particular, strengths of the program included training, system-level security planning, risk assessment, authorization of system connectivity, and continuous monitoring of security controls. However, information security practices were not fully effective to preserve the confidentiality, integrity, and availability of FHFA's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. CG does not consider the deficiencies noted as a significant deficiency under FISMA.[10] However, CG concluded collectively that the deficiencies are significant in the context of the audit objective as defined for performance audits under GAGAS.

The audit identified FHFA's security practices that can be improved. Specifically, FHFA had not:

- Finalized, disseminated, and implemented an organization-wide information security program plan.
- Updated the Agency's information system policies and procedures to completely address all of the components within the control families from NIST SP 800-53 Rev. 3 applicable to the FHFA information system environment.
- Developed, disseminated, and implemented an agency-wide information categorization policy and methodology.
- Implemented adequate procedures for tracking and monitoring weaknesses or deficiencies through POA&Ms.
- Implemented adequate procedures for tracking and monitoring remediation of weaknesses noted from network vulnerability scans.

Addressing these control deficiencies in security practices will strengthen FHFA's information security program and contribute to ongoing efforts to achieve reasonable assurance of adequate security over information resources.

Table four in Appendix II (page 35) of this report summarizes the results of testing performed of the NIST SP 800-53 Rev. 3 controls selected for evaluation, associated with the information security program management controls, the RMF steps, and the related tasks. Our detailed findings are discussed on pages 18-30.

[10] See page 33 in this report for the definition of significant deficiency under FISMA.

Finding 1 - FHFA Needs to Document an Agency-Wide Information Security Program Plan

FHFA has not finalized and disseminated an organization-wide information security program plan as recommended by the NIST SP 800-53 Rev. 3 and the *Federal Housing Finance Agency Program Management Procedures*.

NIST SP 800-53 Rev. 3 control PM-1, *Program Management Information Security Program Plan,* states:

> The organization:
>
> a. Develops and disseminates an organization-wide information security program plan that:
> — Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
> — Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
> — Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
> — Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation;
> b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; and
> c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

The *Federal Housing Finance Agency Program Management Procedures* documented in August of 2010 require the CISO to develop an agency-wide information security program plan. FHFA hired a CISO in February 2011 who has been in the process of developing and finalizing the plan.

The organization-wide security program plan should address information security for the information and information systems that support the operations and assets of the Agency. Without a documented and approved security program plan, there is an increased risk that FHFA personnel are unaware of the organization-wide information security controls applicable to the Agency and common security controls applicable to the Agency's information systems. Furthermore, communication regarding Agency personnel's responsibilities for developing, implementing, assessing, authorizing, and

monitoring those controls may be lacking. Hence, security controls may not be successfully implemented and monitored. This may lead to the lack of effectively implemented countermeasures to protect FHFA's information systems. Without effective security controls in place, the risk is increased that FHFA is unable to protect its critical information and information systems or data transmitted over the network from unauthorized access which may allow unauthorized users to read, add, delete or modify sensitive information.

Recommendation 1: *We recommend that FHFA's CISO finalize the agency-wide information security program plan in accordance with NIST SP 800-53 Rev. 3 requirements, and disseminate and implement the plan.*

Finding 2 - FHFA Needs to Update Its Information Security Policies and Procedures to Address all Applicable NIST SP 800-53 Rev. 3 Components

FHFA information security policies and procedures are documented based on the controls defined by NIST SP 800-53 Rev. 3. The policies and procedures are organized by and cover each of the NIST SP 800-53 Rev. 3 control families. However, FHFA's information system policies and procedures do not completely address the components within NIST SP 800-53 Rev. 3 control families applicable to the appropriate tailored set of baseline controls.

The FHFA information system policies and procedures do not address recommended components from the following NIST SP 800-53 Rev. 3 control families:

- Access Control (AC)
  - AC-2: Account Management
  - AC-19: Access Control for Mobile Devices
- Audit and Accountability (AU)
  - AU-6: Audit Review, Analysis, and Reporting
- Configuration Management (CM)
  - CM-3: Configuration Change Control
  - CM-8: Information System Component Inventory
- Contingency Planning (CP)
  - CP-9: Information System Backup
- Incident Response (IR)
  - IR-4: Incident Handling
- Physical and Environmental Protection (PE)
  - PE-2: Physical Access Authorizations
  - PE-3: Physical Access Control
  - PE-6: Monitoring Physical Access
  - PE-8: Access Records
- Personnel Security (PS)
  - PS-8: Personnel Sanctions
- Risk Assessment (RA)
  - RA-5: Vulnerability Scanning
- System and Information Integrity (SI)
  - SI-4: Information System Monitoring
  - SI-5: Security Alerts, Advisories, and Directives

CG separately communicated the specific controls within each of the NIST control families noted above that were not completely addressed to FHFA management. Some of these included:

- Contingency Planning (CP-9: Information System Backup)
  - Documenting the frequency of conducting backups of information contained in the Agency's information systems;
- Configuration Management (CM-3: Configuration Change Control)
  - Documenting the retention requirements of records for configuration-controlled system changes
- Access Control (AC-2: Account Management)
  - Documenting how group, system, and application accounts should be managed; and
- Incident Response (IR-4: Incident Handling)
  - Documenting coordination of incident handling activities with contingency planning activities.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers,* states:

> Information security policy is an essential component of information security governance—without the policy, governance has no substance and rules to enforce. Information security policy should be based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS) and guidance; and internal agency requirements.

NIST SP 800-12, *An Introduction to Computer Security: A NIST Handbook, Section 5.2.2 Basic Components of Issue-Specific Policy,* states:

> Computer security policies should be introduced in a manner that ensures that management's unqualified support is clear, especially in environments where employees feel inundated with policies, directives, guidelines, and procedures. The organization's policy is the vehicle for emphasizing management's commitment to computer security and making clear their expectations for employee performance, behavior, and accountability.

FHFA developed its information system policies and procedures in 2010 and is in the process of updating the policies and procedures to ensure the procedures completely address the components within the control families from NIST SP 800-53 Rev. 3 applicable to the FHFA information system environment based on NIST guidance for applying the appropriate tailored set of baseline controls. However, these key areas have not been addressed to date.

The purpose of these policies and procedures is to define the agency-wide information security program and practices. Without comprehensive information security policies and procedures, the likelihood is increased that information security may not be addressed throughout the lifecycle of FHFA's information systems. Moreover,

employees and contractors may be performing tasks without clear direction or training, potentially increasing risk that the Agency's information or information systems could be compromised. The result may be the exposure of FHFA's systems and information to unauthorized access, data loss, data manipulation, and system unavailability. In turn, FHFA could be exposed to financial and reputational risk should a breach of the confidentiality, integrity, or availability of sensitive information occur.

***Recommendation 2*:** *We recommend that FHFA's CISO complete the update of the FHFA information system policies and procedures to address all of the applicable baseline controls within the control families from NIST SP 800-53 Rev. 3.*

Finding 3 - FHFA Needs to Develop an Agency-Wide Information Categorization Policy and Methodology

FHFA has not developed, disseminated, and implemented an agency-wide information categorization policy and methodology based on FIPS PUB 199 as recommended by NIST SP 800-53 Rev. 3. According to FIPS PUB 199, information should be categorized according to its information type and can be applicable to information in both electronic and non-electronic form.

NIST SP 800-53 Rev. 3 control RA-2, *Risk Assessment Security Categorization,* states the following regarding information categorization:

> The organization:
>
> a. Categorizes information and the information system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
> b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
> c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

In addition, FIPS PUB 199 states:

> The security category of an information type can be associated with both user information and system information and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system.
>
> Establishing an appropriate security category of an information type essentially requires determining the potential impact for each security objective associated with the particular information type.

Furthermore, NIST SP 800-60 Vol. 1 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories* (NIST SP 800-60 Vol.1 Rev. 1), states:

> FIPS PUB 199 establishes security categories for both information and information systems. Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.
>
> Agencies support the categorization process by establishing mission-based information types for the organization. The approach to establishing mission-based information types at an agency begins by documenting the agency's mission and business areas. In the case of mission-based information, the

responsible individuals, in coordination with management, operational, enterprise architecture, and security stakeholders, should compile a comprehensive set of the agency's lines of business and mission areas. In addition, responsible individuals should identify the applicable sub-functions necessary to accomplish the organization's mission.

Although FHFA has applied FIPS PUB 199 to the categorization of its information systems, FHFA is maturing the process of applying FIPS PUB 199 to also include categorizing FHFA's information in order to develop an agency-wide information categorization policy and methodology as described in NIST SP 800-60 Vol. 1 Rev. 1.

An agency-wide information categorization policy and methodology facilitates data security by identifying and communicating the level of protection in terms of confidentiality, integrity, and availability required for the Agency's information. The lack of an information categorization policy and methodology limits the ability to properly categorize information systems in order to identify and implement appropriate controls and may produce inconsistency in how information is handled, potentially exposing information to theft, compromise or inappropriate use. Ultimately, the lack of an information categorization policy increases the risk that FHFA could suffer a breach of sensitive data which may result in personal harm, loss of public trust, legal liability, or the high costs of handling a breach.

Recommendation 3: *We recommend that FHFA's CIO coordinate with the executive leadership of the Agency to develop, disseminate, and implement an agency-wide information categorization policy and methodology.*

Finding 4 - FHFA Needs to Strengthen Tracking and Monitoring of Weaknesses and Deficiencies in Plan of Action and Milestones

FHFA's POA&M for information systems did not provide for adequate tracking and monitoring of weaknesses or deficiencies in security controls noted as a result of controls assessments during the security and authorization process. The POA&M identifies tasks to be accomplished, the resources required, milestones in meeting the tasks, and the scheduled completion dates for the milestones. The POA&M is used by the Agency to monitor progress in correcting weaknesses. POA&Ms should be updated on an ongoing basis as part of the continuous monitoring process.

The *Federal Housing Finance Agency Plan of Action and Milestones (POA&M) Process* procedures state that system owners/program offices must define scheduled dates of completion for all weaknesses. From a total population of 41 POA&Ms for the GSS, 13 were not assigned a scheduled date of completion.

POA&Ms that were not assigned a scheduled date of completion included the lack of a formal information security program plan, a formal Enterprise Architecture document, a formal Critical Infrastructure Plan, a formal Risk Management Strategy, and a formal Mission/Business Process Definition. These are all key organization-wide information security program management controls as defined by NIST SP 800-53 Rev. 3. These formal documents ensure that security considerations are addressed throughout the lifecycle of the Agency's information systems, including protection of the Agency's information and critical infrastructure, as well as implementing a risk management strategy consistently across the Agency.

Additionally, POA&Ms lacking a scheduled date of completion included weaknesses related to configuration management and remote access controls. If weaknesses in these two areas remain unaddressed, the risk increases for potential exploitation of deficiencies or weaknesses resulting in unauthorized disclosure, use, or modification of FHFA information.

In addition, program offices/system owners did not ensure remedial actions were taken in a timely manner to mitigate risk to information systems under their purview for the GSS, HSPD-12, and xWorks systems as required by the FHFA's *Program Management Procedures*. CG reviewed the POA&M reports for these systems and noted a number of POA&Ms were past due the scheduled date of completion and no further updates were provided. Table 3 below details the results of the analysis performed.

Table 3: Results of POA&M Analysis

System	Total # of POA&Ms	# of Past Due POA&Ms
GSS	41	5
HSPD-12	24	1
xWorks	3	1

It was unclear whether progress was being made to remediate these weaknesses and when they were expected to be completed. The longer the timeframe that weaknesses are not corrected, the greater the risk that the Agency's information and information systems could be exploited for unauthorized purposes.

NIST SP 800-53 Rev. 3 control CA-5, *Security Assessment and Authorization Plan of Action and Milestones,* states:

> The organization:
>
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

NIST SP 800-53 Rev. 3 control PM-4, *Program Management Plan of Action and Milestones Process*, states:

> The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

FHFA *Plan of Action and Milestones Process* procedures states:

> The scheduled date of completion should be determined based on a realistic estimate of the amount of time it will take to allocate the required resources, implement the corrective action(s), and complete all associated milestones.
>
> The scheduled date of completion should include the month, day, and year, and may not be changed after the initial POA&M entry; progress toward completion is tracked through milestones. If the time to correct the weakness extends beyond the original scheduled date of completion, the status of the weakness must be changed to 'delayed,' and reasons for the delay should be noted in the 'Weakness Comment' field. A revised scheduled date of completion must be recorded in the 'Changes to Milestones' column and reasons for the change must be noted in the 'Comments' field.

Although FHFA has documented POA&M procedures, management oversight was lacking to ensure the procedures were followed. When weaknesses are identified, the related risks and corrective actions should be assessed, tracked and monitored, to ensure effective remediation in a timely manner. In the interim, the systems remain susceptible to risks of unauthorized access, viruses, malicious code, and exploitable

vulnerabilities.

Recommendation 4: *We recommend that FHFA's CISO develop, disseminate, and implement a process to monitor compliance with FHFA POA&M procedures.*

Finding 5 - FHFA Needs to Strengthen Remediation of Vulnerability Assessment Weaknesses

The weaknesses noted in the June 8, 2011, vulnerability assessment report for the GSS and the April 21, 2011, vulnerability assessment report for xWorks were not tracked and monitored for remediation. The vulnerability assessment report noted a high number of vulnerabilities for the GSS. These weaknesses were due to the absence of patching and software updates, which indicate significant configuration management issues. In addition, there were a high number of vulnerabilities noted from the scans for the xWorks system. The POA&M reports for both the GSS and xWorks systems did not include tracking and remediation of any vulnerabilities noted from these scans.[11]

NIST Special Publication (SP) 800-53 Rev. 3 control RA-5, *Risk Assessment Vulnerability Scanning,* states:

> The organization:
>
> a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
> b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
> — Enumerating platforms, software flaws, and improper configurations;
> — Formatting and making transparent, checklists and test procedures; and
> — Measuring vulnerability impact;
> c. Analyzes vulnerability scan reports and results from security control assessments;
> d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
> e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

NIST SP 800-53 Rev. 3 control *CA-5, Security Assessment and Authorization Plan of Action and Milestones,* states:

> The organization:
>
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

[11] The Agency recognized underlying problems with its analysis and reporting of high vulnerabilities.

b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Federal Housing Finance Agency Risk Assessment Procedures states:

Vulnerability Scanning – Risk Assessment, (RA-5)

The Senior Information Security Specialist is responsible for conducting and analyzing vulnerability scans and coordinating the remediation activities with the system engineers in accordance with the following procedure:

1. Scan for vulnerabilities in the information systems and applications at least quarterly, whenever new vulnerabilities potentially affecting the system/applications are identified and reported, when directed to do so by the CISO, or when requested by the SO [System Owner].
2. Conduct vulnerability scans using the approved scanning tool or similar scanning tool approved by the CISO.
3. Ensure that the scanning tool is configured with the most current set of plug-ins prior to conducting any vulnerability scans. This ensures that the most current list of known vulnerabilities is used to evaluate the information systems.
4. Maintain detailed records and documentation for vulnerability scans that demonstrates the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).
5. Ensure that the vulnerability scanning process employs techniques that promote interoperability among tools and automates parts of the vulnerability management process by using standards for:
   - Enumerating platforms, software flaws, and improper configurations;
   - Formatting and making transparent, checklists and test procedures; and
   - Measuring vulnerability impact
6. Work with the system engineers to remediate legitimate vulnerabilities as soon as possible but no longer than 30 days after detection.
7. Share information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
8. Prepare detailed and summary Vulnerability Assessment Reports to be included as artifacts in the C&A packages.

Although FHFA has documented procedures addressing remediation of weaknesses observed from vulnerability scans, FHFA management did not place a priority on monitoring the remediation process to ensure the weaknesses noted from the scans

were tracked in the POA&Ms and remediated.

Addressing vulnerabilities in a timely manner limits the opportunity for attackers to exploit vulnerabilities and gain access to sensitive data or otherwise expose FHFA's systems to unauthorized access, data loss, data manipulation, and system unavailability. The vulnerabilities that were not remediated could lead to total system compromise.

Recommendation 5: *We recommend that FHFA's CISO establish controls for tracking, monitoring, and remediating weaknesses noted from the vulnerability scans.*

Appendix I – Objective, Scope and Methodology

The objective of this performance audit was to evaluate the effectiveness of FHFA's information security program and practices, including FHFA's compliance with FISMA and related information security policies, procedures, standards, and guidelines. FISMA requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The FHFA-OIG's methodology for the FY 11 FISMA audit was a programmatic review of FHFA's governance structure related to the implementation and monitoring of FISMA requirements, and how FHFA has applied the NIST's RMF for managing security throughout the lifecycle of their information systems. The FHFA OIG contracted with CG to evaluate FHFA's compliance with FISMA requirements and report on FHFA's IT controls over its implementation of the NIST RMF. Based on the approach outlined by the FHFA-OIG, CG obtained an overview of the FHFA's Office of the Chief Information Officer oversight role in the following areas:

- Organizational Requirements
- Information Security Policies and Procedures
- Risk Assessments
- System Security Plans
- Security Assessment and Authorization
- Security Awareness, Training, and Education
- Security Incident Reporting
- Contingency Planning
- System Configuration Management
- Plans of Action and Milestones

In addition, CG performed an audit of a selection of internal control activities within each of the following six phases of NIST's RMF:

- Categorizing information systems
- Selecting security controls for information systems
- Implementing information system security controls
- Assessing information system security controls
- Authorizing information systems
- Monitoring information system security controls

Accordingly, CG tested program level controls (including security categorization, information system inventory, risk assessment, security planning, security assessment, plan of action and milestones, security authorization, and continuous monitoring) for a subset of FHFA systems to determine whether FHFA executed the six security program phases in accordance with the following key standards and guidelines:

- FIPS Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems* (Security Categorization)
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* (Minimum Security Controls)
- NIST Special Publication (SP) 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (Security Planning)
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (Risk Assessment)
- NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (System Risk Management Framework)
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View* (Enterprise-Wide Risk Management)
- NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Recommended Security Controls)
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans* (Security Control Assessment)
- NIST SP 800-60 Vol. 1 Rev.1, Volume 1: *Guide for Mapping Types of Information and Information Systems to Security Categories* (Security Category Mapping)

The subset of systems tested included the GSS, xWorks, FHFA's official record of supervision activities for the Division of Enterprise Regulation, and HSPD-12, a contractor system that allows credential bearers to be identified in several standard ways including by photographic images printed on identification cards as well as by biometric data (fingerprints), Personal Information Numbers, and other electronic credentials (digital certificates) stored on the card chip.

In order to implement information system security controls as specified by the RMF, policies and procedures for each of the eighteen NIST control families are required. CG performed a detailed review of design for each policy provided and determined whether the policies and procedures, if properly implemented would comply with NIST requirements for each security control family as outlined in NIST SP 800-53 Rev. 3.

CG conducted this audit in accordance with GAGAS issued by the Comptroller General of the United States. Those standards require that audits be planned and performed to

obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objective. CG believes that the evidence obtained provides a reasonable basis for the finding and conclusions included herein, based on the audit objective.

To assist in the audit, CG reviewed prior year reports to identify potential risk areas. The prior year reports CG reviewed include the FHFA's FY 2010 FISMA evaluation[12] and FY 2009 independent audit report on privacy and data protection.[13] CG also reviewed GAO's report on opportunities for improving the Federal Housing Finance Agency's internal controls and accounting procedures,[14] GAO's report on opportunities for improving information system controls,[15] and GAO's financial audit report for FHFA's FY 2009 and FY 2010 financial statements.[16] Additionally, CG reviewed FHFA's policies, procedures and records, and conducted interviews of FHFA employees and contractor personnel.

A significant deficiency under FISMA is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. As required in FISMA (section 3544(c)(3)), agencies are to report any significant deficiency in policy, procedure, or practice as a material weakness in reporting under the Federal Managers' Financial Integrity Act and if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act.

CG does not consider the deficiencies noted in this report to be a significant deficiency under FISMA. However, CG concluded collectively that the deficiencies are significant in context of the audit objective as defined for performance audits under GAGAS. According to these standards,[17] significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the

[12] *Federal Housing Finance Agency Fiscal Year 2010 Independent Auditor's Federal Information Security Management Act (FISMA) Report,* FHFA Audit Report No. 10-A-03-0TIM, September 30, 2010
[13] *FY 2009 Independent Audit Report on Privacy and Data Protection*, Audit Report No. 09-A-01-OCAO/OTIM,
[14] *Management Report: Opportunities for Improvement in the Federal Housing Finance Agency's Internal Controls and Accounting Procedures,* GAO-11-398R, April 29, 2011
[15] *Information Security: Opportunities Exist for the Federal Housing Finance Agency to Improve Controls*, GAO-10-528, April 2010
[16] *Financial Audit: Federal Housing Finance Agency's Fiscal Years 2010 and 2009 Financial Statements*, GAO-11-151, November 2010
[17] Paragraph 7.04, *Significance in a Performance Audit*, GAO-07-731G (07/07), p. 123.

audited program or activity. Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives.

Appendix II – Summary of Controls Tested

Table 4: Results of Audit

	Related NIST SP 800-53 Rev. 3 Control Tested	Results of Audit
Information Security Program	PM-1 Information Security Program Plan	Issue noted. See Recommendation #1
Information Security Policies and Procedures	All NIST SP 800-53 Rev. 3 Controls	Issue noted. See Recommendation #2
NIST Risk Management Framework (RMF):		
RMF Step 1: Categorize Information System		
TASK 1-1: Categorize the information system and document the results of the security categorization in the security plan.	RA-2 Security Categorization	Issue noted. See Recommendation #3
TASK 1-2: Describe the information system (including system boundary) and document the description in the security plan.	PL-2 System Security Plan	No issues noted.
TASK 1-3: Register the information system with appropriate organizational program/management offices.	PM-5 Information System Inventory	No issues noted.
RMF Step 2: Select Security Controls		
TASK 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).	PL-2 System Security Plan	No issues noted.
TASK 2-2: Select the security controls for the information system and document the controls in the security plan.		No issues noted.

	Related NIST SP 800-53 Rev. 3 Control Tested	Results of Audit
TASK 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.	CA-7 Continuous Monitoring	No issues noted.
TASK 2-4: Review and approve the security plan.	PL-2 System Security Plan	No issues noted.
RMF Step 3: Implement Security Controls		
TASK 3-1: Implement the security controls specified in the security plan.	PL-2 System Security Plan	No issues noted.
TASK 3-2: Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).		No issues noted.
RMF Step 4: Assess Security Controls		
TASK 4-1: Develop, review, and approve a plan to assess the security controls.	CA-2 Security Assessments	No issues noted.
TASK 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.		No issues noted.
TASK 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.		No issues noted.
TASK 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.		No issues noted.

	Related NIST SP 800-53 Rev. 3 Control Tested	Results of Audit
RMF Step 5: Authorize Information System		
TASK 5-1: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.	CA-5 Plan of Action and Milestones	Issue noted. See Recommendation #4.
TASK 5-2: Assemble the security authorization package and submit the package to the authorizing official for adjudication.	CA-6 Security Authorization	No issues noted.
TASK 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	RA-3 Risk Assessment	No issues noted.
TASK 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.		No issues noted.
RMF Step 6: Monitor Security Controls		
TASK 6-1: Determine the security impact of proposed or actual changes to the information system and its environment of operation.	CA-7 Continuous Monitoring	No issues noted.
TASK 6-2: Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.		No issues noted.
TASK 6-3: Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.	RA-5 Vulnerability Scanning	Issue noted. See Recommendation #5.

	Related NIST SP 800-53 Rev. 3 Control Tested	Results of Audit
TASK 6-4: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.	CA-7 Continuous Monitoring	No issues noted.
TASK 6-5: Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.		No issues noted.
TASK 6-6: Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.		No issues noted.
TASK 6-7: Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.		No issues noted.

APPENDIX B

FHFA's Comments to FHFA-OIG's Draft Report

Federal Housing Finance Agency
1700 G Street, N.W., Washington, D.C. 20552-0003
Telephone: (202) 414-3800
Facsimile: (202) 414-3823
www.fhfa.gov

September 19, 2011

Mr. Russell Rau
Deputy Inspector General for Audits
Federal Housing Finance Agency
1625 Eye Street, NW
Washington, DC 20006-4001

SUBJECT: FHFA Response to Independent Evaluation of the Federal Housing Finance Agency's Information Security Program - 2011 (Assignment No. AUD-201 1-011)

This memorandum transmits the FHFA's management responses to the recommendations contained in the draft audit report titled, Independent Evaluation of the Federal Housing Finance Agency's Information Security Program 2011 (Assignment No. AUD-201 1-011). The response to each recommendation including corrective actions is identified below.

Finding 1: FHFA Needs to Document an Agency-Wide Information Security Program Plan

FHFA has not finalized and disseminated an organization-wide information security program plan as recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations and the Federal Housing Finance Agency Program Management Procedures (NIST SP 800-53).*

Recommendation 1: We recommend that FHFA's CISO finalize the agency-wide information security program plan in accordance with NIST SP 800-53 Rev. 3 requirements, and disseminate and implement the plan.

FHFA Response: FHFA concurs with this recommendation.

FHFA Actions: A FHFA IT Security Information Security Program Plan has been completed and is currently being reviewed by management. Approval is expected by October 31, 2011.

Finding 2: FHFA Needs to Update its Information Security Policies and Procedures to Address all Applicable NIST SP 800-53 Rev. 3 Components

FHFA information security policies and procedures are documented based on the controls defined by NIST Special Publication (SP) 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations. The policies and procedures are organized by and cover each of the NIST SP 800-53 control families. However, FHFA's information system policies and procedures do not completely address the components within NIST SP 800-53 control families applicable to the appropriate tailored set of baseline controls. The FHFA information system policies and procedures do not address recommended components from the following NIST SP 800-53 control families:

- Access Control (AC) - AC-2, AC-19
- Audit and Accountability (AU) - AU-6
- Configuration Management (CM) - CM-3, CM-8
- Contingency Planning (CP) - CP-9
- Incident Response (IR) - IR-4
- Physical and Environmental Protection (PE) - PE-2, PE-3, PE-6, PE-8
- Personnel Security (PS) - PS-8
- Risk Assessment (RA) - RA-5
- System and Information Integrity (SI) - SI-4, SI-5

Clifton-Gunderson separately communicated the specific controls within each of the NIST control families noted above that were not completely addressed to FHFA management. Some of these controls included:

- Contingency Planning (CP-9: Information System Backup)
  - Documenting the frequency of conducting backups of information contained in the agency's information systems;
- Configuration Management (CM-3: Configuration Change Control)
  - Documenting the retention requirements of records for configuration controlled system changes;
- Access Control (AC-2: Account Management)
  - Documenting how group, system and application accounts should be managed;
- Incident Response (IR-4: Incident Handling)
  - Documenting coordination of incident handling activities with contingency planning activities.

Recommendation 2: We recommend that FHFA's CISO complete the update of the FHFA information system policies and procedures to address all of the applicable baseline controls within the control families from NIST SP 800-53 Rev. 3.

FHFA Response: FHFA concurs with this recommendation.

FHFA Actions: FHFA is currently conducting its annual review of IT security policies and procedures. Management review and approval is expected by February 2, 2012. The OIG findings will be incorporated as necessary in the annual review and update of the IT security policies and procedures.

Finding 3: FHFA Needs to Develop an Agency-wide Information Categorization Policy and Methodology

FHFA has not developed, disseminated and implemented an agency-wide information categorization policy and methodology based on FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199), as recommended by the NIST Special Publication (SP) 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations (NIST SP 800-53). According to FIPS PUB 199, information is categorized according to its information type and can be applicable to information in both electronic and non-electronic form.

Recommendation 3: We recommend that FHFA's CIO coordinate with the executive leadership of the agency to develop, disseminate, and implement an information categorization policy and methodology.

FHFA Response: FHFA concurs with this recommendation. FHFA agrees that an agency-wide policy for categorization of all agency data (e.g., electronic, paper based, etc.) needs to be developed. For electronic data, FHFA has a methodology based on FIPS 199 for categorization of FHFA information systems and data contained and/or processed by the systems. However, for paper documents, FHFA requires a similar data categorization policy. The Office of Technology and Information Management will take the lead for the Agency in developing an agency-wide policy.

FHFA Actions:
FHFA will develop an agency-wide information classification policy which is expected to be completed by September 28, 2012. This policy will require coordination with all FHFA Divisions and Offices.

Finding 4: FHFA Needs to Strengthen Tracking and Monitoring of Weaknesses and Deficiencies in Plan of Action and Milestones

FHFA's Plan of Action and Milestones (POA&M) for information systems did not provide for adequate tracking and monitoring of weaknesses or deficiencies in security controls noted as a result of controls assessments during the security and authorization process. The POA&M identifies tasks to be accomplished, the resources required, milestones in meeting the tasks, and the scheduled completion dates for the milestones. The POA&M is used by the agency to monitor progress in correcting weaknesses. POA&M should be updated on an ongoing basis as part of the continuous monitoring process.

The FHFA Plan of Action and Milestones Process procedures state that system owners/program offices must define scheduled dates of completion for all weaknesses. From a total population of 41 POA&Ms for the General Support System (GSS), 13 were not assigned a scheduled date of completion.

Recommendation 4: We recommend that FHFA's CISO develop, disseminate, and implement a process to monitor compliance with FHFA POA&M procedures.

FHFA Response: FHFA concurs with this recommendation.

FHFA Actions: FHFA will strengthen the POA&M monitoring process and will provide additional POA&M training to system owners responsible for assigning resources and scheduling actions to remediate vulnerabilities. Training will be completed in the March 30, 2012.

Finding 5: FHFA Needs to Strengthen Remediation of Vulnerability Assessment Weaknesses

The weaknesses noted in the June 8, 2011, vulnerability assessment report for the GSS and the April 21, 2011, vulnerability assessment report for xWorks were not tracked and monitored for remediation. The vulnerability assessment report noted a high number of vulnerabilities for the GSS. These weaknesses were due to the absence of patching and software updates, which indicate significant configuration management issues. In addition, there were a high number of vulnerabilities noted from the scans for the xWorks system. The POA&M reports for both the GSS and xWorks systems did not include tracking and remediation of any vulnerabilities noted from these scans.

Recommendation 5: We recommend that FHFA's CISO establish controls for tracking, monitoring and remediating weaknesses noted from the vulnerability scans.

FHFA Response: FHFA concurs with this recommendation. FHFA recognizes that the vulnerability management assessment program requires enhancements which will improve analysis techniques and reporting. The reports provided to the audit team summarized GSS vulnerability data from April 21, 2011 and June 8, 2011 that were comprised of raw vulnerability scanner output in support of system certification and accreditation activities. The raw data was provided to system owners and administrators with a baseline of all detected system vulnerabilities prior to being evaluated by security analysts. This raw data was not necessarily indicative of vulnerability or finding's security impact to FHFA operations due to:

1. The vulnerability severity ratings for the high findings are proprietary to the vulnerability scanning product used during the assessment.
2. The vulnerability scanning product used to generate the raw vulnerability information associates all instances where an asset is void of a patch, update, or hotfix as a high vulnerability. Because the vulnerability scanning product's knowledgebase, which is independent from vendor or product affiliation, is updated as often as hourly, identified vulnerabilities of which patches may not exist at the time of scanning were also included amongst the high-severity findings.
3. There were 20 xWorks servers which were included in the GSS scans resulting in additional high vulnerabilities. This is due to a vulnerability scanning module that scans for deviations in Windows server compliance based on the vulnerability scanner's default Windows server security standards. In these instances, any deviation is scored as a high finding. Compliance checks are focused on configuration-related items such as login-banner text, service configuration, and audit log settings. For xWorks, a default scan policy was used to provide a baseline level of information for system owners and administrators. The findings noted in the report were based solely on raw vulnerability scanner output.

FHFA Actions: FHFA is incorporating enhancements to the vulnerability management program which will improve our ability to analyze, monitor, and track vulnerabilities. These enhancements are expected to be implemented by February 29, 2012.

If you have any questions, please feel free to contact Ralph Mosios, CISO, (202) 414-3829, e-mail: ralph.mosios@fhfa.gov.

Sincerely,

Kevin Winkler
Chief Information Officer

APPENDIX C

FHFA-OIG's Response to FHFA's Comments

On September 19, 2011, FHFA provided a response (Appendix B) to the draft of this report. FHFA concurred with all recommendations made and described actions it plans to take or has taken to address the issues identified in the report (Appendix A). Based on FHFA's response, FHFA-OIG considers the proposed actions sufficient to resolve the recommendations. However, the recommendations will remain open until such time as FHFA-OIG determines that agreed upon corrective actions are completed and responsive. See Appendix D of this report for a summary of management's comments on the recommendations.

In response to recommendation five, FHFA expressed concern about the output of the vulnerability scanning product in use, noting that the raw scanning data would not necessarily be indicative of system security vulnerabilities until it had been further evaluated by security analysts. In this regard, FHFA is taking action to enhance its analysis of vulnerabilities as stated in its response. FHFA-OIG agrees that not all of the numerous potential vulnerabilities identified by the scanning product would require remediation and that analysis of the raw data is an important part of the remediation process. FHFA agreed that the vulnerability management assessment program requires enhancements, which will improve analysis techniques and reporting. Accordingly, FHFA stated it will incorporate enhancements to the vulnerability program intended to improve the ability to analyze, monitor, and track vulnerabilities by February 29, 2012.

APPENDIX D

Summary of Management's Comments on the Recommendations

This table presents the management response to the recommendations in FHFA-OIG's report and the status of the recommendations as of the date of report issuance.

Rec. No.	*Corrective Action: Taken or Planned*	*Expected Completion Date*	*Monetary Benefits*	*Resolved:[a] Yes or No*	*Open or Closed[b]*
1.	A FHFA IT Security Information Security Program Plan has been completed and is currently being reviewed by management.	10/31/2011	$0	Yes	**Open**
2.	FHFA is currently conducting its annual review of IT security policies and procedures, and as necessary will incorporate FHFA-OIG's findings into the annual review and update of the policies and procedures.	02/02/2012	$0	Yes	**Open**
3.	FHFA—in coordination with all divisions and offices—will develop an agency-wide information classification policy.	09/28/2012	$0	Yes	**Open**
4.	FHFA will strengthen the POA&M monitoring process and will provide additional POA&M training to system owners responsible for assigning resources and scheduling actions to remediate vulnerabilities.	03/30/2012	$0	Yes	**Open**
5.	FHFA is incorporating enhancements to the vulnerability management program, which will improve their ability to analyze, monitor, and track vulnerabilities.	02/29/2012	$0	Yes	**Open**

[a] Resolved means – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation; (2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation; or (3) Management agrees to the FHFA-OIG monetary benefits, a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the FHFA-OIG determines that the agreed-upon corrective actions have been completed and are responsive to the recommendations, the recommendations can be closed.

ADDITIONAL INFORMATION AND COPIES

For additional copies of this report:

- Call the Office of Inspector General (OIG) at: 202-408-2544
- Fax your request to: 202-445-2075
- Visit the OIG website at: www.fhfaoig.gov

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

- Call our Hotline at: 1-800-793-7724
- Fax us the complaint directly to: 202-445-2075
- E-mail us at: oighotline@fhfa.gov
- Write to us at: FHFA Office of Inspector General
  Attn: Office of Investigation – Hotline
  1625 Eye Street, NW
  Washington, DC 20006-4001