audit report

Issue Date:
June 12, 2008
Audit Case Number
2008-DP-0004

TO: Brian D. Montgomery, Assistant Secretary for Housing – Federal Housing Commissioner, H
Mike Milazzo, Acting Chief Information Officer, Q

/s/

FROM: Dorothy Bagley, Acting Director, Information Systems Audit Division, GAA

SUBJECT: Review of Selected FHA Major Applications' Information Security Controls

HIGHLIGHTS

What We Audited and Why

We audited the Federal Housing Administration's (FHA) management of its information technology resources and compliance with U.S. Department of Housing and Urban Development (HUD) and other federal information security requirements. Our overall objective was to determine whether FHA effectively managed security controls relating to its information technology resources. This audit supported our financial statement audits of FHA and HUD as well as our annual Federal Information Security Management Act review.

What We Found

FHA did not (1) fully implement required security controls related to personnel security, user access, and audit log management for the Single Family Insurance System - Claims Subsystem; (2) define or implement adequate security controls over its business partners that develop, store, and process HUD data; and (3) have assurance that mandatory security controls had been implemented and follow the federal information security framework.

We also found that the HUD Office of the Chief Information Officer did not follow its own policy on performing security impact assessments when significant changes were made to a system.

What We Recommend

We recommend that FHA and HUD incorporate the federal information security program framework into their management processes so that security assessments, continuous monitoring, personnel security, and appropriate access to systems and data are assured.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

Auditee's Response

The complete text of the auditee's response, along with our evaluation of that response, can be found in appendix A of this report.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

The Federal Housing Administration (FHA) provides mortgage insurance on loans made by FHA-approved lenders throughout the United States and its territories. FHA has developed a number of information systems to support its mortgage insurance and related program activities. We recently evaluated 25 of FHA's major information systems and issued an audit report on the information security weaknesses identified.[1]

The Federal Information Security Management Act of 2002 (FISMA) provides a "comprehensive framework" to ensure that agency information security controls support and protect federal operations and their assets. Compliance with FISMA entails an active management of organizational risk and is the key element in the organization's compliance with the federal information security program framework. The information security framework guides the selection of appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The guidance provided in FISMA details the agency's responsibilities to protect against unauthorized use of information that could harm information collected on behalf of the agency. We used FISMA's requirements as the basis in developing our methodology for performing this audit.

Our overall objective was to determine whether FHA's information system security controls had been fully implemented for selected FHA applications. The criteria that we used during our audit included information security circulars issued by the Office of Management and Budget, FISMA, and publications by the National Institute of Standards and Technology.

[1] Audit Report No. 2008-DP-0002, "Review of FHA Controls over Its Information Technology Resources," dated October 31, 2007.

RESULTS OF AUDIT

Finding 1: Weaknesses Existed in Security Controls for the Single Family Insurance System - Claims Subsystem

Key personnel within FHA (1) did not enforce personnel security policies and ensure that appropriate background investigations were completed for employees and contractors for the Single Family Insurance System - Claims Subsystem, (2) gave excessive access rights and access to data beyond employees' and contractors' job requirements, and (3) did not establish an effective audit log management and monitoring process. FHA officials indicated that they either did not realize the need to have background investigations or assumed that information technology (IT) developers' background investigations had been properly completed. Further, FHA had not implemented effective processes for managing and monitoring system access privileges and audit logs. Without adequate background checks, access rights assignment, and audit log management, FHA did not operate the Claims Subsystem in accordance with federal information security requirements. As a result, the data processed within the Claims Subsystem were not adequately protected.

The Claims Subsystem is one of HUD's mission-critical systems. This major application is used by HUD headquarters and field office personnel, external government agencies, and business partners to electronically submit and process claims for single-family mortgage insurance benefits. The system processes approximately 178,000 claims per year. Payment schedules averaging $25-$30 million per day are transmitted to the U.S. Treasury, with total single-family mortgage insurance benefit payments exceeding $6 billion per year.

Appropriate Background Checks Were Not Performed

FHA employees and contractors did not always have a background investigation or the appropriate background investigation. HUD Personnel Security Handbook 732.2, REV-1, section 4-5B, states, "every HUD employee and every contractor working on behalf of HUD has, on record, no less than National Agency Check and Inquiries (NACI). For those with above-read access to financial systems or other systems designated by the Department a Limited Background Investigation is required." In addition, the matrix for background investigations for financial systems in appendix A of the handbook indicates that the developer and project lead should have a limited background investigation, while supervisors of moderate risk systems and system/security administrators should have a background investigation, the highest investigation type.

In our review of 24 HUD employees and contractors who had above-read access to Claims Subsystem production data files, we identified the following:

- Ten employees did not have a background investigation on file.
- Eleven employees did not have the proper background investigation.
  - Six HUD employees had only a minimum background investigation[2] but should have had a limited background investigation[3] since they all had greater than read access to Claims Subsystem production data files.
  - Five HUD contactors did not have a full background investigation as required for their positions. One of the five was the Endevor [4] administrator who had a limited background investigation rather than the full background investigation required for system/security administrators. The other four had minimum background investigations, although their positions required them to have limited background investigations.
- The remaining three employees had the proper background investigations.

FHA officials indicated that they did not know the employees and contractors did not have a background investigation or did not have the proper background investigations; rather, they assumed that the IT developers' background investigations had been properly conducted. By not performing required background screenings, HUD increased its risk that unsuitable individuals would have access to sensitive systems and data. Background investigations ensure, to the extent possible, that employees are suitable to perform their duties.

[2] According to the HUD Handbook 732.3 REV-1, "Personnel Security/Suitability," a minimum background investigation consists of a National Agency Check and Inquiries (NACI) plus an automated credit check covering residence and employment locations for the past five years, an interview of the subject, and written inquiry of residences, and references. A National Agency Check and Inquiries is the minimum investigation required for all Federal employment, including contractors, except when employment is not to exceed 180 days in the aggregate. It is a background investigation, but is conducted only for individuals in non-sensitive positions and is referred to Government-wide as a NACI.

[3] According to the HUD Handbook 732.3 REV-1, "Personnel Security/Suitability," a limited background investigation is an investigation which consists of a National Agency Check and Inquiries, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years.

[4] Endevor is a configuration management tool that controls, automates, and monitors the entire application development life cycle. An Endevor administrator can control source code files.

Unnecessary Access Rights Were Granted to Production Data Files

Some FHA application developers and Claims Subsystem users had more access to the application's production data files[5] than was necessary to perform their assigned job functions. Specifically,

- Two Claims Subsystem users, a financial analyst and an accountant from the Single Family Accounting Branch, had access type "all" to all the data files, which permitted them to read, write, and update records. Financial analysts and accountants typically do not require access to production data files and are not required to modify them.

- Three application project officers for the Claims Subsystem had update access to a data file but did not require above-read access.

- Five IT contractor developers were granted above-read access to production data files, which violated HUD's policy of not allowing developers access to production resources.

FHA's system owners did not realize that some users had been granted above-read access to Claims Subsystem data files as they had not implemented an efficient monitoring process.

By not following the principle of least privilege, HUD decreased its ability to protect sensitive information and limit the potential damage that could result from accident, error, or unauthorized use. Additionally, HUD risked exposure of confidential and critical information by providing access to applications or system attributes that were above the users' authorized access levels.

Audit Logs Were Not Adequately Managed and Monitored

FHA did not design or implement effective information security controls for monitoring and managing audit logs. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems," states, "The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity,

[5] The HUD General Deputy Assistant Secretary for Administration's memorandum to the Office of Administration Government Technical Representatives and Government Technical Monitors, dated February 28, 2000, states that "HUD will no longer approve requests to provide IT developers with production accounts or allow access to production resources (application systems)."

investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions."

Although, the Claims Subsystem application's audit logs were able to capture and monitor its transactions, the application's user login activities recorded in the Customer Information Control System's[6] audit log had not been sufficiently retained and monitored. HUD stated that these user login data were not reviewed unless there was an incident that required investigation. HUD Handbook 2400.25, REV-1, "Information Technology Security Policy," requires audit logs to be recorded and retained for no less than a year for systems rated moderate to high, the periodic review of audit records for inappropriate or unusual activity, investigation of suspicious activity or suspected violations, and reporting of findings to the appropriate officials.

Without adequate security log management process controls in place, HUD could not maintain an inclusive history of events, and it would be unable to perform audit and forensic analysis and identify operational trends and long-term problems, which could help establish security controls.

Conclusion

FHA did not fully design or implement required information security controls related to background checks, access rights, or audit log management because of the insufficient security control oversight and monitoring at the general support system and application levels. Without these information security controls in place, FHA could not operate the Claims Subsystem, one of its major applications, in accordance with federal information security requirements, and the data processed within the Claims Subsystem were not adequately protected.

Recommendations

We recommend that the Assistant Secretary for Housing

1A. Ensure that FHA system owners work closely with application government technical monitors/government technical representatives to identify and obtain

[6] The Customer Information Control System is a transaction processing system that runs primarily on IBM mainframe systems for online and batch activities and acts as a front-end access to an application (e.g., the Claims Subsystem) and to provide online transaction management connectivity for mission-critical applications.

the appropriate access and background investigations for their application users.

1B. Initiate a request with Office of Security and Emergency Planning staff to determine whether the FHA contractor employees have had the appropriate background investigations. Follow up with Office of Security and Emergency Planning staff to ensure that background investigations are initiated for FHA applications' contractor staff if required.

1C. Obtain the listing of Claims Subsystem users with above-read access to the production data files from the Office of the Chief Information Officer (OCIO) and work with OCIO to make the necessary adjustment to their access privileges based on their job functions.

1D. Obtain the current listing of all users with above-read access to FHA application data from OCIO, perform an assessment to determine specifically what access is granted to all FHA developers including both HUD employees and contractors, and update this listing with the assistance of OCIO to ensure that the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks are assigned.

We recommend that the Acting Chief Information Officer

1E. Provide FHA with a current listing of all users with above-read access to FHA application data and remove any developers' unnecessary access to FHA applications upon FHA's confirmation notification.

1F. Initiate a request with the Office of Security and Emergency Planning staff to determine whether the IT infrastructure contractor employees with administrative access (such as DB2, Endevor, and PVCS) to FHA applications and the platforms where the applications reside have had appropriate background investigations. Follow up with Office of Security and Emergency Planning staff to ensure that background investigations are initiated for IT infrastructure contractor staff if required.

1G. Require the HUD IT infrastructure contractor to maintain the Customer Information Control System audit log that allows the activities to be traced back for at least one year.

1H. Require the HUD information technology infrastructure contractor to provide a Customer Information Control System user failed logon attempts report and then disseminate pertinent information to the information system security officers for review and monitoring on a periodic basis.

Finding 2: FHA Did Not Define or Implement Adequate Security Control Requirements over Business Partner Development, Processing, or Storage of Single-Family Mortgage Data

FHA did not develop or implement adequate information security controls for its business partners and outside entities that remotely access or develop, process, and maintain HUD data for the FHA Connection application. FHA depended on its business partners to generate, process, and store FHA mortgage data but had not established information security guidance or requirements. As a federal entity, FHA is required by FISMA to ensure that its data are adequately protected from unauthorized access, use, destruction, disclosure, disruption, or modification even when the data are maintained on behalf of the agency. FHA program staff were not fully aware of their responsibility for the information collected, processed, and stored on their behalf. By not providing adequate security controls and safeguards over data maintained outside HUD's secured physical perimeter, FHA did not comply with HUD regulations or federal guidelines. As a result, data that were critical to FHA's mission and its ability to operate efficiently and effectively were at risk of theft, loss, or destruction.

Security Controls for Business Partners Were Not Developed or Defined

FHA did not develop or implement adequate security controls over its business partners and outside entities that remotely access or develop, process, and maintain HUD data outside the agency's secured physical perimeter. FHA did not consider or assess the risk of exchanging information among business partners and other external entities or develop appropriate security controls. Based on interviews with FHA officials, there was no FHA-specific process that established specific requirements to protect information exchanged and/or that specified particular remedies for failure to protect the information as prescribed.

We found a lack of management controls over the FHA Connection, an interactive system on the Internet that gives approved business partners and outside entities access to update single-family mortgage and insurance systems. As of April 1, 2008, 59,342 users from 22,425 institutions and branches had signed up to use the FHA Connection, and average volume was between 200,000 and 250,000 transactions per day. FHA management did not (1) provide guidance on required security controls such as data retention and encryption or disposal of confidential and personally identifiable information, (2) require a memorandum of understanding with business partners detailing security requirements, or (3) monitor or require quality assurance reviews of systems that provide data to HUD or data collected, processed, and maintained remotely on behalf of HUD.

FISMA holds federal agencies responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on their behalf and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

NIST SP 800-53[7] states that the assurance or confidence that the risk to the organization's operations, assets, and individuals is at an acceptable level depends on the trust that the authorizing official places in the external service provider. In some cases, the level of trust is based on the amount of direct control the authorizing official is able to exert on the external service provider with regard to the employment of appropriate security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. The level of control is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider) to very limited (e.g., using a contract or service-level agreement).

FHA program managers and system owners did not review or require security controls over FHA's partners because they were not fully aware of the federal requirements to do so. They believed that they should not have to provide guidance, monitor, or require the business partners to implement and maintain security measures.

Further, FHA maintained that there was no way to structurally organize a security policy for all outside personnel that access its systems. Business partners completed a yearly quality controls self-assessment as required by FHA; however, there was no quality assurance requirement for information systems security controls. FHA did not require or plan to address the lack of security controls in the quality control process. As a result, FHA did not monitor the security measures in place at its business partners' sites and did not require assurance regarding the information systems controls that were implemented. Without these assurances, FHA could not fulfill its responsibilities under FISMA related to providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by FHA or on its behalf.

[7] "Recommended Security Controls for Federal Information Systems," dated December 2006.

Conclusion

FHA did not comply with federal statutes or information security requirements, as it did not develop or implement adequate security controls over its business partners and outside entities that remotely access or develop, process, and maintain HUD data outside the agency's secured physical perimeter. This condition occurred because FHA program staff believed that they were not responsible for the information collected, processed, and stored on their behalf. Further, FHA management did not provide sufficient guidance on required security controls and adequately monitor business partner use of systems that provide data to HUD or data collected, processed, and maintained remotely on behalf of HUD. As a result, FHA data were at an unmeasured level of risk of theft, loss, or destruction.

FHA relies heavily on its business partners' and outside entities' use of information technology systems and data to carry out its mission and operate efficiently and effectively. Therefore, appropriate security controls and safeguards must be established to minimize the risks associated with business partners and outside entities remotely accessing, developing, processing, and maintaining HUD data.

Recommendations

We recommend the Assistant Secretary for Housing

2A. Identify the information security controls needed by FHA to ensure that the data uploaded into the FHA Connection are adequately protected and use a risk-based approach that requires its business partners to design and implement appropriate information security controls in their operation.

2B. Design and implement guidance, tools, and the communications necessary to ensure that FHA's business partners are aware of their roles and responsibilities to protect FHA data.

2C. Ensure that within the annual quality assurance requirements, there is a requirement for an assessment of the business partners' information security controls that protect FHA data.

2D. Coordinate the quality assurance plans with business partners to include security measures.

Finding 3: FHA Did Not Have Assurance That Mandatory Security Controls Had Been Implemented

FHA's Office of Housing did not ensure that mandatory security controls[8] that establish a level of "security due diligence" were implemented, assessed, or monitored. Our review of the information security self-assessment[9] documents for several major FHA applications[10] disclosed (1) missing or improperly assigned mandatory security controls, (2) common security controls that were not clearly identified, and (3) a lack of appropriate security awareness and specialized training. These deficiencies occurred because the responsibility for the assessment and monitoring of common controls was not clearly assigned, HUD and federal regulations were misunderstood, and some FHA personnel involved in completing security self-assessments lacked the appropriate role-based training. As a result, HUD and FHA could not ensure that their information systems and data were adequately secured and protected. Lack of understanding the status of security programs and controls prohibits HUD and FHA management from making informed decisions and investments to mitigate risks that can negatively impact their ability to meet mission goals.

Mandatory Security Controls Were Consistently Missing from System Security Documentation

During the Office of Housing's self-assessments completed in September 2007, not all required security controls were assessed. The mandatory security controls were not assessed because they were not a part of the FHA-prepared security control listing or due to the improper impact ratings for the applications.[11] This omission resulted in those specific security controls not being included in the FHA major applications' security documentation and monitoring processes. After the self-assessment process, FHA, independent from the Office of Inspector

[8] Controls are classified as common controls or application-specific controls. Security controls designated by the organization as common controls are in most cases managed by an organizational entity other than the information system owner. Application controls or organization security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives.

[9] The self-assessment questionnaire, based on NIST SP 800-53 controls for information systems, provides the agency baseline of mandatory controls.

[10] Single Family Insurance System - Claims Subsystem , Single Family Acquired Asset Management System, Single Family Mortgage Notes, Home Equity Conversion Mortgages, Computerized Homes Underwriting Management, FHA Connection, and FHA Subsidiary Ledger.

[11] As required by FISMA, the US Department of Commerce's National Institute of Standards and Technology promulgated the Federal Information Processing Standard (FIPS) 199 which establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

General and using contractor support, identified 23 NIST SP 800-53 security controls as missing from FHA's baseline[12] of security controls. The information security controls missing from the entire selected FHA major application security program included

- Security-related activity planning;
- Acquisition;
- Security certification;
- Fire protection;
- Information system backup;
- Information system component inventory (low and moderate baselines);
- Flaw remediation;
- Information system monitoring tool and techniques;
- Media transport (moderate and high baselines);
- Remote access;
- Use of external information system;
- Auditable events;
- Audit monitoring, analysis, and reporting;
- Time stamps;
- Boundary protection (including control enhancements 3, 4, and 5);
- Secure name/resolution service (authoritative service);
- Architecture and provisioning for name/address resolution; and
- Session authenticity.

There were also five security controls that were missing due to the improper impact rating for the application. These lacking security controls applied to those sections that were improperly assigned low, moderate, and high impact.

- Contingency planning control CP-6.2 was not applicable to a moderate system.
- Remote maintenance was missing (from a moderate system).
- Media labeling was not applicable to a moderate system.
- Wireless access restriction was missing (from a moderate system).
- Resource priority was not applicable to a moderate system.

[12] Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization in accordance with FIPS 199.

Common Security Controls Were Not Clearly Identified

Security controls designated by the organization as "common controls" (i.e., controls that are common to FHA and other HUD organizations) are managed by the Office of the Chief Information Officer (OCIO) rather than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. Every control in a baseline must be fully addressed by either the organization or the information system owner.

OCIO's information security self-assessment template is provided to the information systems security officer and system owners as guidance for the assessment of the minimum baseline security controls as outlined in NIST 800-53. The template did not clearly identify which of the template's controls was HUD's responsibility as a common control. This condition adversely impacted FHA's ability to identify the controls it was responsible for on an application level. Consequently, FHA created its own set of information security controls determining which controls were its responsibility and which controls should be the responsibility of OCIO. As a result, mandatory controls were not assessed or monitored.

FHA Staff Required Role-Based Security Awareness and Training

The Office of Housing was taking steps to improve its information technology security awareness and documentation; however, its lack of understanding of mandatory security controls for which it is responsible resulted in a deficient IT security program. Complete self-assessment information and guidance were provided on the HUD internal Web site; however, the proper tools were not used to ensure that all elements of the annual security reviews were completed and implemented. The noted deficiencies were primarily due to a misunderstanding of the regulations. The lack of FHA staff training contributed to these missing elements. Not all staff members who played a pertinent role in completing the security assessment documentation received the same training.

Federal regulations require that individuals with security responsibility have the required training to meet their job functions. NIST SP 800-16, "Information Technology Security Training Requirements: A Role and Performance Model," section 4.1, states, "...training and education are to be provided selectively, based

on individual responsibilities and needs. Specifically, training is to be provided to individuals based on their particular job functions. Education is intended for designated IT security specialists in addition to role based training."

Conclusion

FHA did not comply with HUD and federal regulations with regard to annual security assessments and had no assurance that all mandatory security controls had been implemented. As a result, HUD and FHA could not properly ensure that their information systems and data were adequately secured and protected from threats. The deficiencies identified above occurred because (1) responsibility for the assessment and monitoring of common controls was not clearly assigned, (2) HUD and federal regulations were misunderstood, and (3) all FHA personnel involved in completing security self-assessments did not receive the appropriate role-based training.

It is necessary that officials understand the current status of security programs and controls to make informed judgments and investments that appropriately mitigate risks that could negatively impact their mission goals. FHA needs to ensure that all elements are fully implemented into its security documents to prevent and plan for possible situations and risks associated with the data HUD maintains.

Recommendations

We recommend that the Assistant Secretary for Housing

3A. Ensure that a training development plan is fully implemented so that staff may complete their tasks based on their specific positions and be fully aware of their roles and responsibilities as they relate to the management of the systems.

3B. Monitor and ensure that the missing security controls are implemented in all future security self-assessments, continuous monitoring, activities, and the fiscal year 2008 certification and accreditation process.

3C. Include missing security controls in appropriate system security plans used by the Office of Housing.

We recommend that the Acting Chief Information Officer

3D. Revise the self-assessment template to note which of the controls listed are considered to be common controls and as a result, primarily the responsibility of OCIO as the general support system owner.

Finding 4: HUD OCIO Did Not Follow Its Own Policy on Performing Security Impact Assessments When Significant Changes Were Made

HUD's Office of the Chief Information Officer (OCIO) made a significant change to a general support system[13] that supports FHA's core financial system, the upgrading of an operating system, without performing a security impact assessment as required by federal and HUD information system policy. This situation occurred because HUD's contractor did not consider the change to be significant and advised HUD that a security impact assessment was not needed. To determine whether there was a security impact to the general support system, we performed a series of compliance checks[14] and found a number of improper configurations, mostly related to password issues, and policy violations on associated Windows servers. These vulnerabilities should have been reported and incorporated into HUD's monitoring program until corrected. Without conducting a security impact assessment, OCIO could not assure itself or HUD's components that it had adequately protected HUD's systems.

HUD Did Not Follow Its Own Certification and Accreditation Policy

HUD did not comply with the federal information security framework related to the continuous monitoring phase of the certification and accreditation process. Specifically, HUD did not review significant changes made to a general support system. A significant change imposes a change in the security risks faced and needs to be analyzed by performing a security impact assessment. Our review found that HUD did not complete a security impact assessment of the general support system that supports FHA's core financial system, FHA Subsidiary Ledger, before upgrading the operating system from Solaris version 8 to version 10. Federal guidance specifically identifies operating system changes as significant.

OCIO was not able to provide planning documentation to justify its reasoning prepared in advance of the conversion for not conducting a security impact assessment. OCIO staff stated that they relied on the contractor responsible for HUD's information technology infrastructure and did not believe a security impact assessment or a new certification and accreditation were necessary. They added that there were only a few systems converted to the new updated software

[13] An interconnected set of information resources under the same management control that shares common functionality. It includes hardware, software, information, data, applications, communication, and people.
[14] Unlike scans, which usually involve a more comprehensive vulnerability assessment, a compliance check is a manual check of configurations on the server against configuration guidelines provided by NIST and the Defense Information Systems Agency security technical implementation guidelines.

and that a certification and accreditation would take place sometime in fiscal year 2008.

The federal guidance[15] that governs certification and accreditation states that when accrediting a federal information system, an agency official accepts the risks associated with operating the system and the associated implications regarding agency operations, agency assets, or individuals. Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that there will be a reaccreditation whenever there is a significant change to the system or its operational environment. The guidance specifically states that a change to an operating system is a significant change.

A security impact assessment was not performed when completing changes to the general support system because HUD's information technology infrastructure contractor recommended that a security impact assessment was not needed. OCIO accepted the recommendation from the contractor without documented evidence identifying reasons why a security impact assessment should not be completed. After we questioned OCIO, OCIO staff requested additional information and received a written document from the contractor explaining its recommendation. However, the statement did not conform to either HUD or federal policy.

FHA's core financial system was one of the systems residing on the general support system that migrated from the Solaris 8 operating system to the Solaris 10 operating system, and affected servers processed the financial data that were the source for FHA's financial statement reports. The lack of review before the conversion left this information susceptible to undetected changes.

Improper System Configurations Went Undetected

OCIO did not perform security assessments or testing on the UNIX servers impacted by the conversion from Solaris 8 to Solaris 10 or associated Windows servers to determine whether the new implementation created any new vulnerabilities. Without testing, there would be no way to determine whether any additional controls were needed to address the differences between the two operating systems. We were told that HUD had not prepared standard procedures for the new features in version 10, which could leave data vulnerable. In addition, roles and responsibilities associated with these new features had not been designated.

[15] NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004.

To determine whether a security impact assessment would have identified security violations or improper configurations, we conducted compliance checks on production UNIX and supporting Windows servers. We did not find any critical security violations; however, we did find a number of improper configurations, which should be addressed. We provided OCIO with the results of the compliance checks.

The configuration tests that we completed indicated that there were security violations or improper configurations to the systems that had not been addressed, thereby leaving data and information open to risk. Without a proper security assessment, HUD could not ensure that it had adequately protected its systems that process critical information.

Conclusion

HUD's OCIO did not follow its own or federal policy when it made a significant change to a general support system without performing a security impact assessment. This resulted in security violations and improper configurations that had not been addressed, thereby leaving data and information open to risk. This situation occurred because OCIO accepted its information technology contractor's assertion that a security impact assessment was not needed, although the decision directly contradicted HUD and federal policy. The migration from Solaris 8 to Solaris 10 directly affected servers that housed FHA's core financial system and financial data that were the source for FHA's financial reports. The lack of review before the conversion might have left this information susceptible to undetected changes, which could call into question the validity of the FHA financial statements.

Recommendations

We recommend that the Acting Chief Information Officer

4A. Complete a certification and accreditation of the general support systems that upgraded from the Solaris 8 to the Solaris 10 operating system.

4B. Provide training to system owners, including the general support systems owners, to ensure an understanding of federal regulations and the HUD handbook with regard to significant changes to their systems.

4C. Issue a memorandum to its IT infrastructure contractors reminding them of their contractual obligation to fully comply with HUD security policy and

obtain a signed acknowledgment and complete, at minimum, a security impact assessment of the changes when significant changes are made to general support systems and obtain in writing from the contractors their assurance that they understand and accept this requirement.

SCOPE AND METHODOLOGY

We performed the audit

- From June through December 2007,
- At HUD headquarters in Washington, DC, and
- In accordance with generally accepted government auditing standards.

We reviewed information security documents, Office of Housing major applications, and the general support systems' compliance with federal and HUD information security requirements. We focused on organizational structure and security documents that were created in fiscal year 2007.

We used a selective sampling method to evaluate the compliance of the seven selected Office of Housing major applications from a universe of 40 major FHA applications reported in HUD's system inventory list as of January 19, 2007. The seven major applications were selected because they were managed by the Office of Housing, supported FHA program areas, and were categorized as major applications.

To accomplish our objectives, we reviewed policies and procedures, interviewed FHA system owners for each application, and obtained and analyzed supporting documentation. We also interviewed staff from OCIO, the Office of Integration and Efficiency, and the Office of Housing's Office of Finance and Budget, Office of Systems and Technology, to better understand the structure and organization upon which information security was based in the Office of Housing. These interviews were conducted to determine roles and responsibilities of the system owners from their perspectives and compare them to what is stated in HUD policy. We also conducted compliance checks on production UNIX and supporting Windows servers where major FHA applications reside to determine whether a security impact assessment would have identified security violations or improper configurations.

INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined the following internal controls were relevant to our audit objectives:

- Appropriate level of access to data and systems,
- Compliance with personnel security requirements,
- Design and implementation of information security baseline controls,
- Compliance with certification and accreditation, and
- Compliance with information security assessments.

We assessed the relevant controls identified above.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

Significant Weaknesses

Based on our review, we believe the following item is a significant weakness:

- FHA and HUD's OCIO had not fully integrated the federal information security program framework with their organizational processes to ensure that security documents, continuous monitoring, personnel security, and appropriate access to systems and data were adequate (findings 1, 2, 3, and 4).

FOLLOWUP ON PRIOR AUDITS

Review of FHA Controls over Its Information Technology Resources
Audit Report: 2008-DP-0002
October 31, 2007

The following recommendations from our prior audit remain open:

1A. Design and implement an FHA information security program consistent with HUD and federal requirements to include

i. Designating a senior FHA staff member to lead information technology and security functions within FHA. The FHA security function would be subordinate to HUD's for external reporting and department-wide information security issues but would be able to focus and enhance HUD requirements for FHA-specific needs and risks.

ii. Ensuring that a compliant information security risk-based framework is implemented for all FHA applications.

1B. Direct application system owners to fully assume the roles and responsibilities of system owners in accordance with HUD IT Security Policy - Handbook 2400.25, REV-1.

1C. Mandate a role-based training program for FHA program staff with significant information security responsibilities.

2A. Structure the management authorities relating to information security functions so that they provide the oversight necessary to ensure that information security receives the consideration needed when allocating resources.

2B. Direct application system owners to determine the amount and type of resources needed to ensure adequate security for their systems.

2C. Develop an FHA-wide plan to ensure that the dollar amount and resources are listed in budget requests and that resources are adequate to complete security for their systems.

2D. Revise the HUD standard business impact analysis to include all necessary elements outlined in NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," so that the analysis supports the preparation of the continuity of operations and business resumption plans.

2E. Provide additional guidance and training to application system owners regarding completion of their application's business impact analysis.

3A. Complete the design and implementation of an information security program to include

- Accurate and fully agreed-upon descriptions of program office application system owner roles and responsibilities.
- Documented processes, procedures, or agreements related to the implementation of information security controls with FHA for each general support system on which its applications reside.
- Documenting, in HUD's information technology policy, the use of the Information System Security Forum as a user representative forum for each general support system. The forum could be used to update the security officer on the status of information security policy on the general support systems on which its applications reside.

3B. Develop and provide role-based training to FHA staff with information security roles and responsibilities, including but not limited to

- Application system owners,
- Information system security officers,
- Project managers, and
- Authorizing officials and other staff with management responsibilities for the certification and accreditation process.

3C. Require FHA authorizing officials, information system owners, and information system security officers to obtain the training necessary to assume their information security roles and responsibilities.

APPENDIXES

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation **Auditee Comments**

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-8000

ASSISTANT SECRETARY FOR HOUSING-
FEDERAL HOUSING COMMISSIONER

MEMORANDUM FOR: Dorothy Bagley, Acting Director, Information Systems Audit Division, GAA

FROM: George Rabil, Housing-FHA Comptroller, HW

SUBJECT: Response to OIG Draft Audit Report - Application Control Review of FHA Major Applications

This memorandum is in response to your May 2, 2008, request for comments on the draft audit report on the Application Control Review of FHA Major Applications. We have reviewed the subject report and provide the following general comments. Our detailed comments for each finding and recommendation are attached. We will provide target dates and milestones for implementation, as needed, in our subsequent management decision response.

While Housing-FHA concurs with the recommendations in this audit, we believe a number of issues raised should be addressed at the Departmental level. Also, it should be noted that while Housing-FHA follows the Department's guidance as issued by HUD Office of Security and Emergency Planning, we would recommend the process for personnel security be reviewed and addressed at the Departmental level.

Further, it is appropriate that the Role Based Training be centralized as an Office of the Chief Information Officer (OCIO) function and not within individual program offices. OCIO is the Departments' authority on information technology security policies and guidance; therefore the training should be an enterprise-wide standard and solution. In addition, the training would be in compliance with applicable federal guidelines and more cost effective eliminating the need for program offices to obtain individual contracts to develop and provide training which would place further strains on resources.

We look forward to working with you and your staff to resolve and close-out the recommendations. Should you have any questions or need additional information please contact me at 202-402-3127

Attachment

Auditee's Detailed Comments on Draft Audit Report
Application Control Review of FHA Major Applications
Report Dated 05/02/2008

Draft Report Reference	Assistant Secretary for Housing – Federal Housing Commissioner and Management Comments for OIG's Consideration
Recommendation 1A (page 8) - Ensure that FHA system owners work closely with application government technical monitors/government technical representatives to identify and obtain the appropriate access and background investigations for their application users.	Housing-FHA concurs with this recommendation. Housing-FHA will follow the HUD process and will coordinate with the System Owners and ensure that they work closely with GTM/Rs in obtaining the required background investigations for users or contractors.
Recommendation 1B (page 9) - Initiate a request with Office of Security and Emergency Planning staff to determine whether the FHA contractor employees have had the appropriate background investigations. Follow up with Office of Security and Emergency Planning staff to ensure that background investigations are initiated for FHA applications' contractor staff if required.	Housing-FHA concurs with this recommendation. Housing-FHA will follow the HUD process and initiate an official request through CHAMPS to OSEP. Housing-FHA will work closely with OSEP to ensure that background investigations are initiated and will monitor the CHAMPS requests until completed.
Recommendation 1C (page 9) - Obtain the listing of Claims Subsystem users with above-read access to the production data files from the Office of the Chief Information Officer (OCIO) and work with OCIO to make the necessary adjustment to their access privileges based on their job functions.	Housing-FHA concurs with this recommendation and has completed the recommended actions. The Claims Branch received and reviewed the sub-systems list as requested. The review confirmed that each person named has (1) a valid need to access and (2) the appropriate access "least privilege" based on the individual job functions. Additionally, access was removed via CHAMP request for the two employees who were identified as retirees.
Recommendation 1D (page 9) - Obtain the current listing of all users with above-read access to FHA application data from OCIO. Perform an assessment to determine specifically what access is granted to all FHA developers including both HUD employees and contractors,	Housing-FHA concurs with this recommendation. Housing-FHA will work with OCIO and obtain a current listing of all users with above read access to FHA data application. A thorough review and assessment will be conducted and appropriate action taken.

Comment 1

and update this listing with the assistance of OCIO to ensure that the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks are assigned.	
Recommendation 2A (page 12) - Identify the information security controls needed by FHA to ensure that the data uploaded into the FHA Connection are adequately protected and use a risk-based approach that requires its business partners to design and implement appropriate information security controls in their operation.	Housing-FHA concurs with this recommendation. The Office of Single Family Program Development, as system owner for FHAC, will collaborate with the Office on Lender Activities and Program Compliance on formulating, designing and implementing information security controls for its business partners. There has been initial discussion regarding the best approach to ensuring that security controls are in place for the data uploaded into FHAC, that it is adequately protected, and that it uses a risk-based approach that requires our business partners to design and implement information security controls in their operation. Meetings will be scheduled and we will work until a solution that can be implemented has been developed.
Recommendation 2B (page 12) - Design and implement guidance, tools, and the communications necessary to ensure that FHA's business partners are aware of their roles and responsibilities to protect FHA data	Housing-FHA concurs with this recommendation. There are several possible solutions to ensuring that FHA's business partners are aware of their roles and responsibilities. Possible solutions are not limited to those described below: • Develop a certification process that will be incorporated into the standard documents required for submission to FHA when a new lender is seeking FHA approval status or when an already approved FHA lender completes their annual renewal process. • Develop a standard Rules of Behavior list that will require a new FHAC application coordinator or standard user to certify to prior to receipt of approval to access the system. • Develop a yearly security web based training program that users would be required to view and certify that they completed the course – similar to the course that HUD staff and contractors are required to complete. • Consider use of individual Memorandum of Understanding. This would be a major initiative as

	there are presently over 10,000 FHA-approved lenders. All alternatives will be explored before one or a combination of requirements is issued.
Recommendation 2C (page 12) - Ensure that within the annual quality assurance requirements, there is a requirement for an assessment of the business partners' information security controls that protect FHA data.	Housing-FHA concurs with this recommendation. The annual quality assurance requirements will be modified to incorporate assessment of the business partner's information security controls once the policy guidance has been established.
Recommendation 2D (page 12) - Coordinate the quality assurance plans with business partners to include security measures.	Housing-FHA concurs with this recommendation. Instructions to lenders will be issued requiring updating of their individual internal Quality Control Plans to incorporate information security controls that protect FHA data.
Recommendation 3A (page 16) - Ensure that a training development plan is fully implemented so that staff may complete their tasks based on their specific positions and be fully aware of their roles and responsibilities as they relate to the management of the systems.	Housing-FHA concurs with this recommendation. Housing-FHA is in the process of developing role based training into a training plan that can be implemented before the end of this fiscal year. In addition, Housing-FHA will work closely with OCIO to ensure that the appropriate staff complete the OCIO security training when made available.
Recommendation 3B (page 16) - Monitor and ensure that the missing security controls are implemented in all future security self-assessments, continuous monitoring, activities, and the fiscal year 2008 certification and accreditation process.	Housing-FHA concurs with this recommendation and has completed the recommended actions. Housing-FHA has coordinated with OCIO to ensure that all missing security controls have been incorporated into OCIO's System Security Self Assessments, continuous monitoring activities and the fiscal year 2008 certification and accreditation (C&A) process. Currently C&As are in progress for all major Housing-FHA systems.
Recommendation 3C (page 16) - Include missing security controls in appropriate system security plans used by the Office of Housing.	Housing-FHA concurs with this recommendation and has completed the recommended actions. Housing-FHA has coordinated with OCIO to ensure that all applicable security controls have been incorporated into the OCIO SSP template. Information System Security Officers and System Owners are required to update all SSPs based on the updated template.

Comment 2

Comment 3

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

May 28, 2008

MEMORANDUM FOR: Hanh Do, Director, Information System Audit Division, GAA

FROM: For Mike Milazzo, Acting Chief Information Officer, Q

SUBJECT: Office of Inspector General's Review of Selected FHA Major Applications' Information Security Controls (DP-07-0016)

This memorandum is in response to your May 2, 2008 draft audit report entitled, "Review of Selected FHA Major Applications' Information Security Controls." As you know, my staff has worked closely with your staff on the notifications of findings and recommendations for this audit.

The Office of Information Technology (IT) Security, Office of Systems Integration and Efficiency, and the Office of IT Operations have carefully reviewed the report and are providing the following comments on the report and its recommendations in the attached matrix. The matrix shows the implemented corrective action taken to date, as well as the planned corrective actions that will be taken to effectively implement and close the recommendations.

It is my understanding that the final report will reflect all of these comments. We look forward to working with you and your staff to resolve and close out the recommendations.

In the interim, should you have any questions or need additional information, please contact Shelia Fitzgerald, Audit Liaison Officer, at ext. 2432.

Attachments

Comment 4

Comment 5

OCIO's Program Management Responses to
OIG Application Control Review of Selected FHA Major Application
DP-07-0016

Recommendations Applicable to OCIO	Program Management Response
1E. Provide FHA with a current listing of all users with above-read access to FHA application data and remove any developers' unnecessary access to FHA applications.	ECD: POC: H. Zarrinnahad OCIO conditionally concurs with this recommendation. Implemented Corrective Action(s): Planned Corrective Action(s): OCIO conditionally concurs with the recommendation for the following reasons: Any action/s OCIO takes is contingent upon FHA's full cooperation for consolidation and reconciliation. Justification must be provided by FHA/Housing for allowing the developer access to application systems. Once this happens, OCIO will then be able to remove developers' unnecessary access to FHA production applications.
1F. Initiate a request with the Office of Security and Emergency Planning staff to determine whether the IT infrastructure contractor employees with access to FHA applications have had appropriate background investigations. Follow up with Office of Security and Emergency Planning staff to ensure that background investigations are initiated for IT infrastructure contractor staff if required.	ECD: POC: M.Gibbs OCIO concurs with this recommendation. Implemented Corrective Action(s): Planned Corrective Action(s): OCIO ISSO will verify that GSS infrastructure contractor system administrators have background investigations initiated, as recommended in OIG audit 2008-DP-0003 3B. OCIO will also ensure that infrastructure contractor staff who support DB2, Endeavor and PVCS activities have background

1

	investigations initiated. OCIO will provide a worksheet with names and actions taken (if any).
1G. Require the HUD IT infrastructure contractor to maintain the Customer Information Control System audit log that allows the activities to be traced back for at least one year.	ECD: POC: M.Gibbs OCIO concurs with this recommendation. Implemented Corrective Action(s): The OCIO has implemented longer retention periods for Customer Information Control System audit logs. Planned Corrective Action(s): At the time that OCIO has one year's worth of logs, OCIO will provide documentation.
1H. Require the HUD information technology infrastructure contractor to provide a Customer Information Control System user failed logon attempts report and then disseminate pertinent information to the information system security officers for review and monitoring on a periodic basis.	ECD: POC: M. Gibbs OCIO concurs with this recommendation. Implemented Corrective Action(s): Planned Corrective Action(s): The OCIO ISSO will share Customer Information Control System (CISC) user failed logon attempts information with the CICS ISSO on a periodic basis or as needed.
3D. Revise the self-assessment template to note which of the controls listed are considered to be common controls and as a result, primarily the responsibility of OCIO as the general support system owner.	ECD: POC: John Smith OCIO concurs with this recommendation.

Comment 6

OCIO's Program Management Responses to
OIG Application Control Review of Selected FHA Major Application
DP-07-0016

	Implemented Corrective Action(s): Common controls have been discussed with ISSOs during ISSO forums in FY 2008. Planned Corrective Action(s): The self-assessment template will be updated to note which controls listed are considered to be common controls on the OCIO IT Security website.
4A. Complete a security impact assessment and a certification and accreditation of the general support systems that upgraded from the Solaris 8 to the Solaris 10 operating system.	ECD: POC: Harold Williams OCIO non-concurs with this recommendation. Implemented Corrective Action(s): The certification and accreditation process is on-going. The C & A is the total process. The security impact assessment is excessive when a C & A is performed. Therefore, the OIG should remove the security impact assessment requirement. Planned Corrective Action(s): We will complete a C & A process for that general support system covering all components that have been upgraded from Solaris 8 to Solaris 10. The deadline for completion of C & As for the general support systems is November 2008.
4B. Provide training to system owners, including the general support systems owners, to ensure an understanding of federal regulations and the HUD handbook with regard to significant changes to their systems.	ECD: POC: B. Blunt OCIO concurs with this recommendation.

3

OCIO's Program Management Responses to
OIG Application Control Review of Selected FHA Major Application
DP-07-0016

	Implemented Corrective Action(s): Planned Corrective Action(s): To ensure an understanding of federal regulations and the HUD handbook with regard to significant changes to their systems, role-based training program will be provided to system owners and the general support systems owners.
4C. Issue a memorandum to EDS and Lockheed Martin reminding them of their contractual obligation to fully comply with HUD security policy and complete, at minimum, a security impact assessment of the changes when significant changes are made to a GSS and obtain in writing from the contractors their assurance that they understand and accept this requirement.	ECD: POC: J.Svatek OCIO concurs with this recommendation. Implemented Corrective Action(s): The HITS GTR notified the HITS vendors, via email, reminding them of their contractual obligation to fully comply with HUD security policy and to complete security impact assessments for major changes to the GSS. Planned Corrective Action(s): The OCIO will obtain written confirmation/acceptance from the HITS vendors.

OIG Evaluation of Auditee Comments

Comment 1 OIG agrees with FHA's implemented corrective actions as stated. OIG also requests that supporting documentation and the completion dates be provided in order to confirm complete implementation of this recommendation. Once confirmed, no further correction action is necessary from FHA and this recommendation can be closed.

Comment 2 OIG agrees with FHA's implemented corrective actions. OIG also requests that supporting documentation and the completion dates be provided in order to confirm complete implementation of this recommendation. Once confirmed, no further correction action is necessary from FHA and this recommendation can be closed.

Comment 3 OIG agrees with FHA's implemented corrective actions as stated. OIG also requests that supporting documentation and the completion dates be provided in order to confirm complete implementation of this recommendation. Once confirmed, no further correction action is necessary from FHA and this recommendation can be closed.

Comment 4 OIG has revised the recommendation to reflect that the action OCIO is to carry out is contingent "upon FHA's confirmation notification."

Comment 5 OIG has made minor revisions to this recommendation based on discussions with OCIO.

Comment 6 OIG reevaluated the recommendation based on OCIO's comments and has revised the recommendation accordingly.