



Issue Date	March 4, 2008
Audit Report Number	2008-DP-0003

TO: John W. Cox, Chief Financial Officer, F
Mike Milazzo, Acting Chief Information Officer, Q
Brian D. Montgomery, Assistant Secretary for Housing – Federal Housing
Commissioner, H
Keith Nelson, Assistant Secretary for Administration, A
/s/
FROM: Dorothy Bagley, Acting Director, Information Systems Audit Division, GAA

SUBJECT: Fiscal Year 2007 Review of Information Systems Controls in Support of the
Financial Statements Audit

HIGHLIGHTS

What We Audited and Why

We reviewed general and application controls for selected information systems to assess management controls over the U.S. Department of Housing and Urban Development's (HUD) computing environments as part of the Office of Inspector General's (OIG) audit of HUD's financial statements for fiscal year 2007 under the Chief Financial Officer's Act of 1990.

What We Found

HUD did not ensure that its general and application controls over its financial systems conformed to federal requirements and guidelines. Specifically, HUD did not ensure that (1) adequate application controls for its financial systems were in place and operating effectively, (2) file and configuration management controls in the IBM z/OS environment were fully implemented, and (3) controls over information technology personnel security practices were fully implemented and minimized risks of unauthorized access to its systems. As a result, HUD's financial systems were at risk of compromise.

What We Recommend

We recommend that the Office of the Chief Financial Officer strengthen the application controls for HUD's financial systems and ensure that access to sensitive financial data is restricted to those who have a specific business need.

We recommend that the Office of the Chief Information Officer provide logs and listings to assist the program offices in ensuring that users' system access levels are commensurate with their position and supported by appropriate background investigation.

We recommend that the Assistant Secretary for Housing ensure that contractor support staff review and update Federal Housing Administration application configuration management documentation and ensure that unnecessary files are removed from the IBM mainframe environments in a timely manner.

We recommend that the Office of Security and Emergency Planning update policies and procedures, and revise the HUD personnel security and suitability handbook to clarify ambiguous and contradictory information with regard to background investigations, position sensitivity, and risk levels.

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 auditees' responses, along with our evaluation of those responses, can be found in appendixes A through D of this report.

TABLE OF CONTENTS

Background and Objectives	4
Results of Audit	
Finding 1: Insufficient Application Controls over HUD’s Financial Systems Posed a Risk of Unauthorized Access to Financial Data	5
Finding 2: File and Configuration Management Controls in the IBM z/OS Environment Were Inadequate	12
Finding 3: Personnel Security Practices Continued to Pose a Risk of Unauthorized Access to HUD Systems	16
Scope and Methodology	20
Internal Controls	22
Follow-up on Prior Audits	23
Appendixes	
A. OCFO’s Comments and OIG’s Evaluation	24
B. OCIO’s Comments and OIG’s Evaluation	31
C. FHA’s Comments and OIG’s Evaluation	34
D. OSEP’s Comments and OIG’s Evaluation	36

BACKGROUND AND OBJECTIVES

The Government Management Reform Act of 1994 amended the requirements of the Chief Financial Officers Act of 1990 by requiring the annual preparation and audit of federal agency financial statements. The methodology for performing financial statement audits is provided in the “Financial Audit Manual,” which was jointly developed by the General Accountability Office and the President’s Council on Integrity and Efficiency. This manual explains that the overall purposes of performing financial statement audits of federal entities include providing decision makers (financial statement users) with assurance as to whether the financial statements are reliable, internal control is effective, and laws and regulations are complied with.

The effectiveness of internal controls over computer-based information systems is the subject of this audit. Our objective was to evaluate general and application controls over financial systems that support U.S. Department of Housing and Urban Development (HUD) business operations. We followed the methodology outlined in the General Accountability Office’s “Federal Information System Controls Audit Manual” for evaluating internal controls over the integrity, confidentiality, and availability of data maintained in computer-based information systems. We focused on the effectiveness of general controls over HUD general support systems¹ on which the financial applications function and the specific controls directly associated with selected individual financial applications (application controls²). These information system controls can affect the security and reliability of not only financial information, but also other sensitive data (e.g., employee personnel data, the public housing inventory, and housing tenant family data) maintained on the same general support systems. Specifically, we reviewed general controls for the IBM mainframe operating system, application controls for selected HUD financial systems, and personnel security controls.

The criteria that we used during our audit included the Federal Information Security Management Act, Office of Management and Budget circulars, and National Institute of Standards and Technology publications.

¹ A “general support system” or “system” is defined in Office of Management and Budget Circular A-130, appendix III, as “an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).”

² Application controls are directly related to individual computerized applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

RESULTS OF AUDIT

Finding 1: Insufficient Application Controls over HUD's Financial Systems Posed a Risk of Unauthorized Access to Financial Data

HUD did not ensure that adequate application controls for its financial systems were in place and operating effectively. We noted the following deficiencies: (1) controls over the Line of Credit Control System (LOCCS) user recertification process were not effective to ensure that all users were properly recertified, (2) a contractor had unauthorized access to sensitive data on the Financial Data Mart, (3) all users with access to the HUD Web had inappropriate access to and could generate reports containing proprietary financial data maintained within the Financial Data Mart, (4) contractors with access to HUD Central Accounting and Program System (HUDCAPS) production data did not receive the required level of background investigation, and (5) HUD did not document either its acceptance of the risk associated with or the justification for contractors/developers granted above-read access to the production data for the HUDCAPS application. These weaknesses existed because sufficient policies and procedures had not been implemented to ensure that National Institute of Standards and Technology (NIST) and HUD guidelines were followed. Further, management was not aware of all requirements associated with granting access to the financial systems. By not limiting, reviewing, and removing inappropriate access authorizations in a timely manner and performing required background screenings, HUD increased its risk that sensitive financial data could be modified, disclosed or misused or that unsuitable individuals could have access to sensitive systems and data.

LOCCS User Recertification Process Did Not Include All System Users

Controls over the LOCCS³ user recertification process were not effective in ensuring that all users were properly recertified. HUD Handbook 2400.25, section 5.1, Identification and Authentication, requires that user access be reviewed once a year. Of the 23,826 LOCCS application users, 10,079 did not have a date of last user recertification in the system, indicating that their system access had not been reviewed and validated. Of these users, 8,401 were classified as an approver. The approver access level allows the user to recertify the access granted to regular users within the LOCCS application. The remaining 1,678

³ The Line of Credit Control System (LOCCS) supports the Office of the Chief Financial Officer (CFO) and all HUD Program Offices in coordinating and controlling grant, loan, and subsidy disbursements. The system is the CFO's primary vehicle for cash management while monitoring disbursements per the individual control requirements used by HUD Program Offices to ensure program compliance. LOCCS can make check payments and wire transfer funds to recipients. LOCCS utilizes Automated Clearing House (ACH) payment mechanisms to make wire transfer payments.

users included 1,592 users listed as grantees, who were authorized to draw money from the system, and 86 regular HUD users authorized to enter/modify data within the system.

Many of the 1,678 users may have been dual users of the system at one time. Dual user is defined as a user granted both regular (data entry) and approver-level access within the application. LOCCS was not designed to identify dual users by user type categorization. A separate user classification to identify this type of user had not been created, and the user type that was reflected on the record for dual users was not accurate.

We also identified 199 users whose last recertification date was before March 31, 2006, indicating that they had not been included in the recertification process. By not ensuring that the access levels of all LOCCS users had been reviewed, HUD was unable to ensure that users only had access to the data within the core financial systems that were necessary for them to complete their jobs, that only authorized users had access to the system, and that users who no longer required access to the data in the system no longer had access to the system. Additionally, the Office of the Chief Financial Officer could not produce accurate reports regarding user access to LOCCS.

Financial Data within the Financial Data Mart Were Inappropriately Accessed

HUD had not taken adequate steps to control access to proprietary financial data contained in the Financial Data Mart⁴. Specifically,

- A contractor gained unauthorized access to sensitive data contained in the Financial Data Mart using a software application's login identification (ID) and password. The software application's login ID was designed to allow testing in the application development environment for a program used to generate reports from the Financial Data Mart production data. The individual indicated that no data within the Data Mart were reviewed. However, it is not possible to prevent a user with access to the production data from viewing or generating screen prints of the data. HUD Handbook 2400.25, REV 1, section 5.3, Audit and Accountability,

⁴ The Financial Data Mart was created to provide a consolidated reporting environment of HUD's financial data to users to create ad hoc queries and reports for analysis and execute canned financial reports. The Financial Data Mart stores information from several separate systems, including: HUDCAPS (HUD's main accounting system), PAS (a legacy accounting system that still performs some of HUD's accounting functions), LOCCS (HUD's Line of Credit Control System), NLS (HUD's Nortridge Loan System), HPS (HUD's Procurement System) and DLA (Defense Logistics Agency).

requires program offices/system owners to “develop and implement a process to periodically review audit records for inappropriate or unusual activity.” The handbook further requires that an automated mechanism be used in the review of audit records for systems rated moderate or high and that audit records related to users with significant system roles and responsibilities be reviewed more frequently. However, an effective process to review audit logs had not been implemented.

HUD Handbook 2400.25, REV 1, section 5.3.1, Passwords, defines a strong password as one with “a minimum of eight alphanumeric characters with a least one uppercase letter, one lower case letter, one digit, and one special character. Strong passwords do not have common words or permutations of the user name.” The password assigned to the software application’s login ID did not conform to HUD’s password policy. The application’s password was less than eight characters long, used only lowercase letters, contained a portion of the user ID name, and did not include special characters or numbers. There was no mechanism in place to enforce HUD’s password policy.

- All users with access to the HUD Web could access and generate reports containing proprietary financial data maintained within the Financial Data Mart. The information available from the Web site included financial data related to grantees, public housing agencies, and individual program areas as well as the Office of Inspector General (OIG). NIST Special Publication (SP) 800-53, REV-1, appendix F, AC-6, Least Privilege, requires that an information system rated moderate or high enforce the most restrictive set of rights/privileges or accesses needed by users for the performance of their assigned tasks.

The unlimited access was provided to allow HUD program managers, budget officers, financial analysts, accountants, and users of Office of the Chief Financial Officer systems to obtain reports on financial data and to reduce the volume of printed reports previously provided via legacy applications. However, access was not limited to those users who required such access to accomplish their job duties, and the security risk associated with unlimited access to proprietary financial data was not adequately assessed. By not limiting access to users solely for the performance of their assigned tasks, HUD increased the risk that the sensitive, proprietary data maintained in the Financial Data Mart could be inappropriately disclosed or misused. This could result in harm to either HUD or other individuals/business partners whose data are maintained within the Financial Data Mart.

Developers with Access to HUDCAPS Production Data Did Not Receive Proper Background Investigations

HUD did not take steps to ensure that information technology contractors were properly screened before being granted access to sensitive systems and application data in accordance with HUD and NIST guidelines. Specifically, we identified two developers who had above-read access to the HUDCAPS⁵ production data but were not properly screened. One developer received only a minimum background investigation. The other developer was not screened at all. An OIG audit report detailing similar background investigation weaknesses was issued on February 22, 2007.⁶

HUD Personnel Security Handbook 732-3, chapter 4, section 4.5–B, states that every HUD employee and every contractor working on HUD’s behalf should have on record no less than a national agency check and inquiries (NACI). This is the minimum investigation required for all federal employment, including contractors. For those with above-read access to financial systems or other systems designated by HUD, a limited background investigation is required. The limited background investigation consists of a NACI, credit search, personal subject interview, and personal interviews by an investigator of the subject’s background during the most recent three years.

Background investigations ensure, to the extent possible, that employees are suitable to perform their duties. However, the Office of the Chief Financial Officer did not ensure that contractor employees were properly screened before being granted access to sensitive systems and application data in accordance with HUD and NIST guidelines. By not performing required background screenings, HUD increased its risk that unsuitable individuals would have access to sensitive systems and data.

Contractor Access to HUDCAPS Production Data Was Not Properly Supported

Contractors/developers were granted above-read access to production data for the HUDCAPS application; however, HUD did not document either its acceptance of the risk associated with or the justification for this access level. We identified two contractors/system developers that were granted above-read access to the

⁵ HUDCAPS is the Department’s core financial system. It captures, reports, controls, and summarizes the results of the accounting processes including budget execution and funds control, accounts receivable and collections, accounts payable, and general ledger.

⁶ Audit Report No. 2007-DP-0004, “Fiscal Year 2006 Review of Information Systems Controls in Support of the Financial Statements Audit,” dated February 22, 2007.

HUDCAPS production data stored within the mainframe environment. However, documentation to support this access was not maintained by the system owner, and acceptance of the risk was not documented in the system security plan.

A September 5, 2000, memorandum from the Office of the Chief Information Officer required that system owners and system security administrators accept the risk of granting read-only access to production systems and that their acceptance of that risk must be specifically stated in the system security plan. Further, system owners were required to maintain a file of documentation containing the justification for read access by specific job function and the authorization. During special processing (such as annual close), additional access was temporarily granted for a short period, usually over a weekend. However, follow up reviews were not performed to ensure that the temporary access was removed. Developer access to production systems jeopardized HUD's ability to ensure integrity, confidentiality, and availability of its data and increased the opportunity for fraud.

Conclusion

Without adequate application controls over HUD's financial systems, such as reviews of user access levels and audit logs, limiting access to those users who require such access to accomplish their job duties, performing required background screenings, and ensuring that temporary access to financial systems is removed, HUD could not be assured that (1) users only had access to the data within the core financial systems that were necessary for them to complete their jobs, only authorized users had access to the system, and users who no longer required access to the data in the system no longer had access to the system; (2) sensitive financial data were not inappropriately modified, disclosed, or used; and (3) unsuitable individuals would not have access to sensitive systems and data.

Recommendations

We recommend that the Office of the Chief Financial Officer

- 1A. Strengthen controls over the LOCCS recertification process to
 - Implement a user recertification process that will allow users with approver access within the LOCCS application to be recertified at least annually.
 - Establish a separate user type classification for users granted dual (both approver and regular data entry) access to the LOCCS application.

- Review all user access to the LOCCS application and revise user type classifications when necessary to accurately reflect the current access granted to each user.
- 1B. Develop a process to review audit logs on a regular basis to detect improper, unauthorized system access and use.
 - 1C. Review and update, as needed, all application passwords to ensure that they conform to HUD's password policy.
 - 1D. Restrict access to the Financial Data Mart to those individuals with a defined job-related need to access the data and implement access controls including individual authentication and password protection for the proprietary financial data maintained within the Financial Data Mart.
 - 1E. Perform an assessment to determine specifically what HUDCAPS access is granted to each contractor, and prepare a listing of all users with above-read access to application data. Initiate a request with the Office of Security and Emergency Planning staff to determine whether the contractor employees have had the appropriate background investigations. Follow up with Office of Security and Emergency Planning staff to ensure background investigations are initiated for contractor staff if required.
 - 1F. Initiate action to remove above-read access privileges for all contractors/system developers with unnecessary access within production databases for HUDCAPS and any other Office of the Chief Financial Officer systems.
 - 1G. Develop and maintain files containing the authorizations and justifications for read or above-read access to production data granted to contractors/system developers by the Office of the Chief Financial Officer.
 - 1H. Assess the risk of granting contractors read and above-read access to production data.
 - 1I. Update system security plans to
 - Identify the contractor positions that require read access and the specific instances in which above-read access for contractors/system developers should be requested and/or authorized.
 - Specify the risks associated with granting contractors above-read access to production data and formally accept the risk associated with these access levels.

We recommend that the Office of the Chief Information Officer

- 1J. Provide the Office of the Chief Financial Officer with electronic audit logs to aid in detecting any unauthorized access to the Financial Data Mart servers.
- 1K. Provide the Office of the Chief Financial Officer with a listing of all users with access rights to the HUDCAPS production environment (A75P) to assist in reconciling user access levels with the appropriate background investigations.
- 1L. Remove above-read access privileges for all users within the production databases for HUDCAPS or any other OCFO application environment in accordance with the requests submitted by the Office of the Chief Financial Officer. Provide the Office of the Chief Financial Officer with confirmation that the requested removals have been accomplished.

Finding 2: File and Configuration Management Controls in the IBM z/OS Environment Were Inadequate

HUD did not ensure that (1) all configuration management⁷ documentation was kept up-to-date, (2) unused data files in the IBM mainframe environment were removed in a timely manner, and (3) references to a retired application were removed. Lack of specific requirements, as well as insufficient coordination among different offices prevented HUD from effectively managing its IBM z/OS mainframe environment. As a result, inadequate file and configuration management controls increased the risk that (1) outdated policies and plans might not address current risk and, therefore, be deemed ineffective; (2) programs and program modifications might not be properly authorized, tested, and approved and that access to and distribution of programs might not be carefully controlled; and (3) personally identifiable information could be inappropriately disclosed.

Configuration Management Documentation for Various FHA Applications Was Outdated

Configuration management plans, which are a required part of HUD's system development methodology documentation, did not follow HUD's configuration management guidance. We reviewed the configuration management plans of the Credit Alert Interactive Voice Response System, the Single Family Neighborhood Watch, and the configuration management plan created by Electronic Consulting Services, Incorporated (Electronic Consulting Services). The configuration management plan is shared by five HUD Federal Housing Administration (FHA) applications: (1) Single Family Insurance System, (2) Single Family Insurance Claim System (CLAIMS), (3) Single Family Housing Enterprise Data Warehouse, (4) Consolidated Single Family Statistical System, and (5) Single Family Default Monitoring System. Each plan lacked or contained outdated information for the areas of user access maintenance, configuration management user access verification and deactivation, obsolete module control, and emergency release procedures.

This condition occurred because HUD's system development methodology did not include a specific requirement to review configuration management plans annually and/or to review them when a major change occurred. Further, government technical monitors were not requested to direct the application contract support staff to make the updates. According to the Government Accountability Office's "Federal Information System Control Audit Manual,"

⁷ Configuration management is the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.

section SP-2.2, “To be effective, the policies and plan should be maintained to reflect the current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the type and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees.”

Data and Personal Files No Longer in Use Were Not Removed from the IBM z/OS Environment in a Timely Manner

Policies and procedures for the management of unused data files in the IBM mainframe environment need to be improved. We identified instances in which unused data and personal files were not removed in a timely manner. Specifically,

- The Departmental Platform and Processing Division did not remove 4,144 data files from the development and production environments of the Single Family Insurance Claim System (CLAIMS/A43C). The files were previously used for testing but were no longer needed. Many of these data files contained personally identifiable information such as Social Security numbers. The original request for removal was made in October 2005, but action was not taken until our recent inquiry. This condition occurred because although the file deletion request was made in October 2005, it was not submitted to Departmental Platform and Processing Division release request mailbox.
- The personal data files of three departed contractors were not removed from the IBM development and production environments at the time their user accounts were deleted. Additionally, the personal data files of one retired user were deleted more than a year after the retirement. The data files contained grant information. Also, the personal data files for the top secret administrator, who departed in July 2007, had not been deleted. These personal data files contained information on users, applications, and top secret maintenance programming codes. These conditions occurred because deletion of departed users’ accounts and their personal data files was not always executed at the same time.
- References to a retired application were not removed. The Central Reporting System was retired on September 26, 2000. However, this application’s profile ACIDs,⁸ data files qualifier, and job ID continued to be referenced by

⁸ Profile ACID: CA-Top Secret (the security software used to control and monitor who can access and change data through individual accountability and access permissions and a comprehensive audit trail) defines a set of identical resources’ access authorization once and then associates the entire set with each of the users in a group. This set of

other system profile ACIDs. This condition occurred because the current support vendor was not aware that the Central Reporting System was retired.

Office of Management and Budget Memorandum M-06-15, “Safeguarding Personally Identifiable Information,” points out that the loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. The memorandum reemphasizes federal agency responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information.

NIST Handbook 800-53, “An Introduction to Computer Security,” section AC-2, Account Management, explains that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secure. For systems rated moderate or high impact, inactive accounts should be automatically disabled within a specifically defined period, and automated mechanisms should be used to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified. In addition, section PS-4, Personnel Termination, notes that when employment is terminated, the organization should terminate information system access, conduct exit interviews, ensure the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensure that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.

Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. By obtaining direct access to data files, an individual could make unauthorized changes for personal gain or obtain sensitive information.

Conclusion

Absent updated documentation, HUD risks that (1) outdated policies and plans might not address current risk and, therefore, be deemed ineffective; (2) programs and program modifications might not be properly authorized, tested, and approved and that access to and distribution of programs might not be carefully controlled; and (3) organizational strategic directions and resources assignments for the implementation could not be adequately provided. By not removing data and personal files that may contain sensitive, personally identifiable information in a timely manner, HUD increased its risk that such data could be inappropriately

common resource access characteristics is termed a “profile.” Every profile is assigned a unique profile ACID. ACIDs are the accessor IDs by which users are identified to CA-Top Secret.

disclosed. References to retired application files could render application controls ineffective.

Recommendations

We recommend that the Office of the Chief Information Officer

- 2A. Update its system development methodology to include specific requirements to annually review configuration plans and update them when changes occur.
- 2B. Establish a standard procedure for the removal of the personal data files of users that have departed the agency to include procedures for monitoring and overseeing completion of the removal of the data files.
- 2C. Ensure that the personal data files belonging to the deleted user IDs from IBM mainframe environments are removed, and follow up to verify that the actions have been completed.
- 2D. Run the batch job that will be provided by the CLAIMS contractor to remove the CLAIMS application's unused data files from the IBM mainframe production environment.
- 2E. Ensure that all references to the retired application Central Reporting System are removed.

We recommend that the Assistant Secretary for Housing

- 2F. Ensure that contractor support staff review FHA application configuration management documentation at least annually and update the documentation when changes occur.
- 2G. Update FHA's configuration management documents to remove references that are obsolete and/or no longer applicable and add all missing information.
- 2H. Verify that all unused CLAIMS data files on the IBM mainframe development environment have been removed, and notify government technical monitors of the need to submit file deletion requests to the Departmental Platform and Processing Division release request mailbox.
- 2I. Follow up and verify that the Office of the Chief Information Officer has removed all departed users' personal data files from both production and development environments.

Finding 3: Personnel Security Practices Continued to Pose a Risk of Unauthorized Access to HUD Systems

HUD's information technology personnel security practices continued to pose risks of unauthorized access to its systems. Specifically, (1) contractors had been granted access to sensitive systems without a record of proper background investigations, (2) quarterly user reconciliations did not include all users, and (3) position sensitivity and risk levels for some positions were inconsistent with their levels of responsibility. These conditions occurred because reconciliations designed to identify users that do not have appropriate background investigations did not include users of general support systems. Further, background investigation records maintained by HUD were incomplete. Granting people access to general support systems without appropriate background investigations increases the risk that unsuitable individuals could gain access to sensitive information, use it inappropriately, or destroy it.

For several years, we have reported that HUD's personnel security practices regarding access to critical and sensitive systems were inadequate. Various deficiencies in HUD's information technology personnel security program were found, and recommendations were proposed to correct the problems noted. However, the risk of unauthorized access to HUD's financial systems remains a critical issue.

Contractors Were Inappropriately Granted Access to Sensitive Systems

HUD's information technology contractors were not always screened before being given access to systems and/or networks processing sensitive information. HUD Security Handbook, section 4.1, Personnel, states, "Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems under their purview without having a favorably adjudicated background Investigation, as defined in HUD's Handbook 732.3, Personnel Security/Suitability." HUD was unable to provide the background investigation status for nine contractor personnel supporting its general support systems. Those contractors had high-risk-level positions ranging from system administrators to network engineers and database administrators.

Contractors supporting HUD's network and general support systems did not always have the appropriate level of 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." Appendix A of the handbook identifies

positions such as system administrator and security administrator as high risk and requires that a full background investigation be performed for these positions. We identified 31 information technology contractors who had above-read access but did not have the appropriate level of background investigation. The positions these contractors held included database administrator, network engineer, telecommunications analyst, and system administrator.

This condition occurred because management did not verify that required background investigations had been completed. HUD performed a reconciliation of user access and background investigation records. However, the reconciliation process did not include users with access to general support systems. As a result, the contractors identified above were not included in the reconciliation. Further, personnel records maintained by the Office of Security and Emergency Planning were incomplete. Additionally, users sometimes circumvented prescribed procedures for obtaining system access by legitimately obtaining read access and then going directly to the system administrator to have that access level upgraded, bypassing established controls. Granting people access to general support systems without appropriate background investigations increases the risk that unsuitable individuals could gain access to sensitive information, use it inappropriately, or destroy it.

Quarterly User Reconciliations Did Not Include All Users

Reconciliations to identify users with above-read (query) access to HUD mission-critical (sensitive) applications but without appropriate background checks were conducted. However, the general support systems on which these mission-critical applications reside were not included in the reconciliations because they were not classified as mission-critical. Having access to general support systems typically includes access to system tools, which provide the means to modify data and network configurations.

As noted above, we identified information technology personnel, such as database administrators and network engineers, who had access to these types of system tools but did not have appropriate background checks. These persons were inappropriately excluded from the reconciliation process because they did not have above-read access to mission-critical applications. HUD Handbook 732.3, "Personnel Security/Suitability," chapter 4, section 4-10, states that all access rights must be periodically reviewed to determine whether access is still required. Personnel security controls, such as screening individuals in positions of trust, are particularly important when the risk and magnitude of potential harm is high. Background investigations help an organization to determine whether a particular individual is suitable for a given position by attempting to determine the person's trustworthiness and appropriateness for the position.

Position Sensitivity and Risk Levels Were Inconsistent with Position Responsibilities

Background investigations for HUD information technology contractors were not always performed at the required level. Appendix A of HUD Handbook 732.3, REV-1, "Personnel Security/Suitability," identifies positions such as system administrator and security administrator as high risk and requires that a full background investigation be performed for these positions. We identified 25 information technology contractors with only minimum background investigations who held high-risk positions such as system administrator.

This condition occurred because HUD Handbook 732.3, REV-1, contains ambiguous and contradictory information. For instance, section 3-2, Categories of Sensitive Positions, notes that high-risk positions have significant involvement with one or more mission-critical computer systems and require a full background investigation, while moderate-risk positions have substantial involvement with one or more mission-critical systems and require a limited background investigation. Appendix A of the handbook requires system and security administrators to have full background investigations because of the sensitivity and risk level of those positions. However, section 4-5 of the handbook states, "For those with above read access to financial systems or other systems designated by the Department a Limited Background Investigation (LBI) is required." Many of the information technology contractors did not have direct access to financial systems. Instead, they had full access to the general support systems on which the financial applications operated. Having access to the general support systems typically includes access to system tools, which provide the means to modify data and network configurations.

Granting access to general support systems without appropriate background investigations increases the risk that unsuitable individuals could gain access to sensitive information and use it inappropriately or destroy it.

Conclusion

Without adequate personnel security practices, inappropriate users might be granted access to HUD's information and resources, which could result in destruction or compromise of critical and sensitive data. HUD's information technology personnel security practices continued to pose a risk and HUD could not be sure that unauthorized or unsuitable users were not granted above-read access.

Recommendations

We recommend that the Office of the Chief Information Officer

- 3A. Evaluate position sensitivity and risk levels for information technology contractors to ensure that the classifications are in line with the responsibilities of their positions.
- 3B. Develop a plan to determine whether appropriate background investigations have been conducted for information technology contractors supporting general support systems.

We recommend that the Office of Security Emergency and Planning

- 3C. Coordinate with the Office of the Chief Information Officer and initiate background investigations for those information technology contractors identified as not having a background investigation or only having a NACI on record. Using the listing of contractors with above-read access to financial application data to be provided by the Office of the Chief Financial Officer (as mentioned in recommendation 1E on page 10 of this report), determine whether the contractors have had the appropriate background investigations and initiate necessary investigations.
- 3D. Update policies and procedures to include users of HUD's general support systems in the user access reconciliation process.
- 3E. Revise the HUD personnel security and suitability handbook to clarify ambiguous and contradictory information with regard to background investigations, position sensitivity, and risk levels.

SCOPE AND METHODOLOGY

We performed the audit

- From March through September 2007;
- At HUD headquarters in Washington, DC; the data center in Lanham, Maryland; the data center in West Virginia; and the SunGard disaster recovery facilities in Pennsylvania; and
- In accordance with generally accepted government auditing standards.

Our review was based on the Government Accountability Office's "Federal Information System Controls Audit Manual" and information technology guidelines established by the Office of Management and Budget and the National Institute of Standards and Technology. These publications contain guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data. We evaluated information systems controls intended to

- Protect data and application programs from unauthorized modification, loss, and disclosure;
- Prevent the introduction of unauthorized programs or changes to application and system software;
- Provide segregation of duties involving application programming, system programming, computer operations, information security, and quality assurance;
- Ensure an adequate, entity-wide information security planning and management program; and
- Ensure recovery of computer processing operations in case of disaster or other unexpected interruption.

To evaluate these controls, we identified and reviewed HUD's policies and procedures, conducted tests and observations of controls in operation, and held discussions with HUD staff and contractors to determine whether information systems controls were in place, adequately designed, and operating effectively. In addition, we reviewed corrective actions taken by HUD to address deficiencies identified in prior years' audits.

We also performed audit work in support of this audit, which is included in separate audit reports that have already been issued:

- Audit Report No. 2007-DP-0007, "Network Vulnerability Assessment," issued September 19, 2007

- Audit Memorandum No. 2007-DP-0801, “OIG Response to Questions from the Office of Management and Budget under the Federal Information Security Management Act of 2002,” issued September 28, 2007
- Audit Report No. 2008-DP-0801, “Review of Unisys Performance and Security Controls,” issued October 19, 2007
- Audit Report No. 2008-DP-0002, “Review of FHA Controls over Its Information Technology Resources,” issued October 31, 2007
- “Review of HUD’s Fiscal Year 2007 Information Security Program,” a draft audit report to be issued in March 2008

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:

- System software controls over the IBM z/OS mainframe and Unisys operating systems,
- Access security controls to protect the systems and network from inappropriate and unauthorized access,
- Planning and management of the entity-wide security program, and
- Data center operations controls for contingency and disaster planning.

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 items are significant weaknesses:

- HUD did not have a system to ensure that controls and practices would protect its critical and sensitive systems and computing environments against unauthorized access (findings 1, 2, and 3).

FOLLOW UP ON PRIOR AUDITS

**Fiscal Year 2006 Review of Information
Systems Controls in Support of the
Financial Statements Audit: 2007-DP-0004**

The following recommendations remain open:

- 1D. Ensure that the HITS [HUD's information technology services] contract clearly identifies which contractor should be responsible for the Windows-based applications' production releases, PVCS® Tracker, and Unix-based TeamStudio installations to maintain these services in an efficient manner.
- 1H. Annually update the HUD Procurement System configuration management plan to include (1) the correct version number of PVCS® version manager, server name, and location; (2) removal of the obsolete module section; and (3) a HUD official's approval of the document to ensure that it is in accordance with HUD's department-wide configuration management policies and procedures.
- 1I. Ensure that all procurement system new releases are provided the proper and correct HUD Application Release Tracking System instructions and release version number.
- 1J. Ensure that all procurement systems' modules have been promoted properly by following PVCS® promotion procedures outlined in the "HUD Configuration Management Procedures" document.
- 4B. Remove greater-than-read access to sensitive systems for users who have not submitted appropriate background investigation documents or who are no longer employed by EDS or authorized to access information resources.



APPENDIXES

Appendix A

OCFO's COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

	U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT Washington, DC
CHIEF FINANCIAL OFFICER	
	February 12, 2008
MEMORANDUM FOR:	Dorothy Bagley, Audit Director, Information Systems Audit Division, GAA
FROM:	John W. Cox, Chief Financial Officer, F 
SUBJECT:	Draft Audit Report Fiscal Year 2007 Review of Information Systems Controls in Support of the Financial Statements Audit
<p>This memorandum is in response to your January 14, 2008, request for written comments on the subject draft report. Attached are Office of Chief Financial Officer (OCFO) comments on Finding I and related recommendations 1A- 1I, that were directed to the OCFO.</p> <p>If you have any questions, please contact Keith C. Zahner, Deputy Assistant CFO for Systems, on 202-402-3752.</p>	
Attachment	

**Comments to OIG Draft Audit Report:
Fiscal Year 2007 Review of Information Systems Controls in Support of the Financial
Statements Audit, dated January 14, 2008**

Finding 1: Insufficient Application Controls over HUD's Financial Systems Posed a Risk of Unauthorized Access to Financial Data.

Recommendation 1: We recommend that the Office of the Chief Financial Officer strengthen the application controls for HUD's financial systems and ensure that access to sensitive financial data is restricted to those who have a specific business need. Specifically:

Recommendation 1A: Strengthen controls over the LOCCS recertification process to:

- Implement a user recertification process that will allow users with approver access within the LOCCS application to be recertified at least annually.
 - OCFO does not agree with the recommendation to require an annual recertification of approving officials that do not otherwise have user rights to LOCCS. It is neither practical nor necessary, and it does not improve existing controls.
- Establish a separate user type classification for users granted dual (both approver and regular data entry) access to the LOCCS application.
 - The OCFO does not believe it would be fiscally prudent to expend limited working capital funds to modify LOCCS when a report already identifies the individuals as "Dual Users".
- Review all user access to the LOCCS application and revise user type classifications when necessary to accurately reflect the current access granted to each user.
 - OCFO believes it would be better to handle the "Dual User" classification as a reporting modification rather than an internal LOCCS code modification.

Recommendation 1B: Develop a process to review audit logs on a regular basis to detect improper, unauthorized system access and use.

- In discussions with OIG staff, OIG stated that this recommendation related to the Financial Data Mart. OCFO agrees with the recommendation and has included the review of application-level audit logs as part of the bi-weekly Financial Data Mart status meetings. The application-level audit logs provide metrics relating to User Name and date when the user accessed the OCFO Report Portal. Once OCIO provides the electronic audit logs to OCFO as recommended by OIG (Recommendation 1J), OCFO will include these during the same review.

Comment 1

Comment 2

Comment 3

Comment 4

Comment 5

Recommendation 1C. Review and update, as needed, all application passwords to ensure that they conform to HUD's password policy.

- OCFO agrees with the finding and recommendation and will review and update, as needed, application passwords to ensure they conform to HUD's password policy. Because this may require software changes, and there are limited funds, it may take some time to implement.

Recommendation 1D. Restrict access to the Financial Data Mart to those individuals with a defined job-related need to access the data and implement access controls including individual authentication and password protection for the proprietary financial data maintained within the Financial Data Mart.

OCFO strongly disagrees with this recommendation and the related finding sections based on the following:

Comment 6

- OIG states in Finding 1 on page 5 paragraph 1 "We noted the following deficiencies:(3) all users with access to the HUD Web had inappropriate access to and could generate reports containing proprietary financial data maintained within the Financial Data Mart". This statement is inaccurate and highly misleading as the referenced users accessing HUD Web do not have inappropriate access and cannot create reports. NIST does not define or discuss "proprietary" nor does NIST AC-6 Least Privilege require restriction to information systems based on interpretations of "proprietary". Nevertheless, the general read access referenced in this finding is limited to authorized sources within the HUD firewall, and does not include access to any Privacy Act, Trade Secrets or other moderate or high risk data that could reasonably be construed as "proprietary." Since this statement is inaccurate, OCFO requests that it be deleted.

Comment 7

- OIG also states on page 7 paragraph 3, "The information available from the Web site included financial data related to grantees, public housing agencies, and individual program areas as well as the Office of the Inspector General." On page 7 paragraph 4 it is stated "This could result in harm to either HUD or other individuals/business partners whose data are maintained within the Financial Data Mart". The Web site does not disclose information related to grantees, public housing authorities, or other HUD recipients as stated by the OIG. Since this statement is inaccurate, OCFO requests that it be deleted.

Comment 8

- The limited information available to unlicensed FDM users is not considered sensitive, nor proprietary, and is viewed as low risk. The access to this non-sensitive information has been available since the inception of the FDM. Neither OCFO nor OIG has viewed this issue as either moderate or high risk concern since the inception of the FDM, and no problems have been experienced. The impact of the risk of the unlicensed users accessing the FDM data is LOW since they cannot create reports and access FDM tables containing sensitive information, and in fact, the benefit of accessing this information aids the Department in achieving improved financial management. OCFO has updated the FDM Risk Assessment document to reflect this as LOW risk.

Comment 9

Recommendation 1E. Perform an assessment to determine specifically what HUDCAPS access is granted to each contractor, and prepare a listing of all users with above-read access to application data. Initiate a request with the Office of Security and Emergency Planning staff to determine whether the contractor employees have had the appropriate background investigations. Follow up with Office of Security and Emergency Planning staff to ensure background investigations are initiated for contractor staff if required

- OCFO agrees with the finding and recommendation. Once OCIO has provided a listing of user access rights to the HUDCAPS production environment, OCFO will perform an assessment and initiate a request to OSEP to ensure that contractor employee background investigations have been done. OIG recognizes this responsibility in OCIO Recommendation 1K and in OSEP Recommendation 3C, both revised after February 8 meeting between OIG, OCIO, and OCFO.

Comment 10

Recommendation 1F. Initiate action to remove above-read access privileges for all contractors/system developers with unnecessary access within production databases for HUDCAPS and any other Office of the Chief Financial Officer systems.

- OCFO agrees with the finding and recommendation and will initiate action. Once the request to remove access has been made by OCFO, it is the responsibility of OCIO staff to process the requested action and provide confirmation back to OCFO. OIG recognizes this responsibility in Recommendation 1L, revised after February 8 meeting between OIG, OCIO, and OCFO.

Comment 11

Recommendation 1G. Develop and maintain files containing the authorizations and justifications for read or above-read access to production data granted to contractors/system developers by the Office of the Chief Financial Officer.

- OCFO does maintain files containing the authorizations and justifications for read or above-read access to production data granted to contractor/system developers. OCFO utilizes email communication to support request to OCIO security staff to establish temporary access for contractors to support final annual close processing in HUDCAPS. OCFO's requests are explicit as to who, what files, and for how long. Since the ultimate access change resides at the infrastructure level we (OCFO) do not have access, nor can we verify what was done or undone. OCIO security staff will need to address this control issue.

Comment 12

Recommendation 1H. Assess the risk of granting contractors read and above-read access to production data.

- OCFO agrees with the finding and recommendation. OCFO is currently updating the HUDCAPS risk assessment which will address this issue.

Recommendation 1I. Update system security plans to:

Comment 13

- Identify the contractor positions that require read access and the specific instances in which above-read access for contractors/system developers should be requested and/or authorized.
- Specify the risks associated with granting contractors above-read access to production data and formally accept the risk associated with these access levels.
 - OCFO agrees with the finding and recommendation. OCFO is currently updating application security plans which will address this issue.

OIG'S Evaluation of OCFO's Comments

- Comment 1** Although the OCFO maintains that it is not necessary to annually recertify approving officials that do not otherwise have user rights to LOCCS, by not recertifying these individuals there is no way to verify that they have only the approval authority. LOCCS cannot distinguish users with more than one type of access to the application. As a result, the recertification process currently in place just ignores these users.
- Comment 2** Contrary to the OCFO's assertion, there is no report that identifies dual users. During the audit, the OCFO unsuccessfully attempted to generate reports from LOCCS that identified dual users. None of the reports provided by the OCFO were able to detail the access that current or former dual users have within the LOCCS application. Currently, that information is only available by reviewing the history field of each individual user's security screen in LOCCS. To obtain the information, a person must review the security screen for each user.
- Comment 3** As stated in our response to comment 2, there is no report within LOCCS that details the access granted to a user with dual access to the application. During the audit, because the OCFO was unable to generate reports detailing the access granted to dual users, the OIG was invited to visit the OCFO offices to review the history field of the LOCCS security screen for each individual user.
- Comment 4** The OIG commends the OCFO for taking immediate action on this recommendation.
- Comment 5** The OIG agrees with the OCFO's comments related to this recommendation.
- Comment 6** Allowing all users with access to the HUD Web to also access financial data within the Financial Data Mart violates the concept of least privilege and is therefore inappropriate. Users with access to this data have both the ability to generate reports through the print function and also, the ability to copy the information. While we agree with the OCFO's statement that NIST policies related to least privilege do not require restriction based upon interpretations of proprietary, we disagree with their assertion that the data within the reports is not proprietary. The reports within the Financial Data Mart specifically identify the data as coming from proprietary accounts.
- Comment 7** The Financial Data Mart does disclose financial data related to grantees, public housing authorities or other HUD recipients. Funds are also clearly distinguished by individual program areas, including the Office of the Inspector General.
- Comment 8** The assertion that the OCFO has determined the risk to be low does not mitigate the fact that the access is inappropriate. HUD is required to limit the amount of information that it provides to employees and contractors based upon the concept of least privilege. HUD is required to limit the information provided to employees and contractors to that information needed to perform their specific job

function. A large percentage of the employees and contractors working at HUD do not need to know the specific budget and spending information of organizations within HUD or its business partners. The majority of the HUD staff has no work elements or job components that require them to have access to the financial information that is currently available to them within the Financial Data Mart.

Comment 9 The OIG commends the OCFO's willingness to work in cooperation with the OCIO and OSEP.

Comment 10 The OIG agrees with the comments of the OCFO.

Comment 11 Although requested during the audit, the OCFO did not provide files containing authorizations and justifications for contractors/system developers to have read or above-read access to production data. Once the OCFO provides this information to the OIG, this recommendation can be closed.

Comment 12 The OIG commends the OCFO for their immediate action on this recommendation.

Comment 13 The OIG concurs with the OCFO's response to this recommendation.

Appendix B

OCIO's COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments




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

CHIEF INFORMATION OFFICER

FEB 1 2008

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

FROM:  FOR
Walter Harris, Acting Chief Information Officer, Q

SUBJECT: Comments to the Draft Audit Report on the Fiscal Year 2007
Review of Information Systems Controls in Support of the
Financial Statements Audit (FISCAM)

This memorandum is in response to your January 14, 2008, draft audit report on the Fiscal Year 2007 Review of Information Systems Controls in Support of the Financial Statements Audit. My staff has reviewed the draft report and our comments are provided on the attached.

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 Shelia Fitzgerald, Acting Director, Office of Investment Strategies, Policy and Management at 402- 8063.

Attachment

Detailed Comments on the FY 2007 Review of Information Systems Controls in Support of the Financial Statements Audit (FISCAM)

Comment 1

Comment 2

Comment 3

Draft Report Reference	Office of the Chief Information Officer (OCIO) and Management Comments for OIG's Consideration
2007-DP-XXXX Page 11	<p>Recommendation 1K - Provide the Office of the Chief Financial Officer with a listing of all HUDCAPS users, including contractors, and their access rights to the application to assist in reconciling user access levels with the appropriate background investigations.</p> <p>OCIO does not concur that this is an OCIO action. OCIO recommends this recommendation be assigned to the CFO for resolution by the HUDCAPS system administrator who maintains the application user list.</p>
2007-DP-XXXX Page 11	<p>Recommendation 1L - Remove temporary above-read access privileges of all contractors/system developers within production databases for HUDCAPS and any other Office of the Chief Financial Officer systems in accordance with the duration specified in the original access requests.</p> <p>OCIO does not concur that this is an OCIO action. OCIO recommends this recommendation be assigned to the CFO for resolution by the HUDCAPS system security administrator who has the authority to grant/revoke HUDCAPS access.</p>
2007-DP-XXXX Page 20	<p>Recommendation 3A - Evaluate position sensitivity and risk levels for information technology contractors to ensure that the classifications are in line with the responsibilities of their position.</p> <p>OCIO concurs with this recommendation, as long as it is limited to the evaluation of HUD Information Technology Services (HITS) contractors.</p>

OIG'S Evaluation of OCIO's Comments

Comment 1 OIG met with OCIO representatives on February 8, 2008. During that meeting, OIG and OCIO agreed on the following revision to recommendation 1K: "Provide the Office of the Chief Financial Officer with a listing of all users with access rights to the HUDCAPS production environment (A75P) to assist in reconciling user access levels with the appropriate background investigations."

Comment 2 OIG met with OCIO representatives on February 8, 2008. During that meeting, OIG and OCIO agreed on the following revision to recommendation 1L: "Remove above-read access privileges for all users within the production databases for HUDCAPS or any other OCFO application environment in accordance with the requests submitted by the Office of the Chief Financial Officer. Provide the Office of the Chief Financial Officer with confirmation that the requested removals have been accomplished."

Comment 3 OIG agrees with the OCIO's comment.

Appendix C

FHA's 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

FEB 1 2008

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

FROM: 
George Rabil, Housing-FHA Comptroller, HW

SUBJECT: Response to OIG Draft Report – Fiscal Year 2007 Review of Information Systems Controls in Support of the Financial Statements Audit

Comment 1

We have reviewed the subject report and generally agree with the findings and recommendations addressed to the Assistant Secretary for Housing. During our meeting with your staff on Thursday, January 17, 2008, to discuss the draft report and its related Notice of Findings and Recommendations, we provided comments.

Inasmuch as our comments have been addressed in the revised draft, we have no additional comments. If you have any questions or need additional information, please contact me at 202-402-3127.

OIG'S Evaluation of FHA's Comments

Comment 1 OIG agrees with FHA's comments.

Appendix D

OSEP's COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

**OSEP COMMENTS TO DRAFT AUDIT REPORT –
Fiscal Year 2007 Review of Information Systems Controls
in Support of the Financial Statements Audit**

Comment 1

Comment 2

No	Reference (page, paragraph, sentence)	Audit Report Statement (quote from draft audit)	OSEP Comment
1	Page 20, recommendation 3C	"Coordinate with the Office of the Chief Information Officer and initiate background investigations for those information technology contractors identified as not having a background investigation or only having a NACI on record".	IT will work with OSEP on identifying contractors, who do not have NACI on record (or who have "more-than-read" access to "sensitive" system/s and either have no investigation or only an NACI), and ensure that the appropriate Security Administrator initiates the background investigation forms and submits them to OSEP for forwarding to OPM for initiating a background investigation.
2	Page 20, recommendation 3D	"Update policies and procedures to include users of HUD's general support systems in the user access reconciliation process".	This is part of the Handbook update. 3 (Note: We, in Personnel Security lack the basic knowledge to identify that in the Handbook, except to say that HUD's general support systems automatically are sensitive – if that is correct. More importantly, we reconcile whatever lists are furnished us by CIO.)

OIG'S Evaluation of OSEP's Comments

Comment 1 OIG agrees with OSEP's comment.

Comment 2 OIG confirmed during the audit and in subsequent meetings that persons with above-read access to general support systems were not included in the reconciliations performed by OSEP. In updating HUD's Personnel Security Handbook, it is expected that the revised language will clearly indicate that all access rights must be reviewed, including those with access to general support systems.