



Issue Date February 22, 2007

Audit Report Number 2007-DP-0004

TO: Lisa Schlosser, Chief Information Officer, Q
Joseph A. Neurauter, Chief Procurement Officer, N
Keith A. Nelson, Assistant Secretary, Administration, A

FROM: 
Hanh Do, Director, Information Systems Audit Division, GAA

SUBJECT: Fiscal Year 2006 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 HUD's computing environments as part of the Office of Inspector General's (OIG) audit of the U.S. Department of Housing and Urban Development's (HUD) financial statements for fiscal year 2006 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. Proper configuration management controls for software and document changes are not always employed, and access controls and support for the IBM mainframe operating system console are inadequate. Physical security controls over computing operations facilities are weak, and personnel security practices continue to pose the risk of unauthorized access to HUD systems. As a result, HUD's financial systems are at risk of compromise.

What We Recommend

We recommend that the chief information officer, chief procurement officer, and assistant secretary for the Office of Administration ensure that Office of Management and Budget requirements, Federal Information Security Management Act requirements, National Institute of Standards and Technology guidelines, and HUD's own internal policies and procedures are implemented.

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	4
Results of Audit	
Finding 1: Weaknesses Exist in Configuration Management Support and Practice	5
Finding 2: Access Controls and Support for the IBM Mainframe z/OS Operating System Were Not Adequately Provided	12
Finding 3: Weaknesses Exist in Physical Security Controls over HUD's Computing Operations Facilities	17
Finding 4: Personnel Security Practices Continue to Pose a Risk of Unauthorized Access to HUD Systems	20
Scope and Methodology	24
Internal Controls	25
Follow-up on Prior Audits	26
Appendixes	
A. Auditee Comments and OIG's Evaluation	27

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 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. 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 and application controls for the IBM mainframe operating system and Windows-based HUD Procurement System as well as personnel and physical security controls.

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

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).”

RESULTS OF AUDIT

Finding 1: Weaknesses Exist in Configuration Management Support and Practice

HUD did not always employ proper configuration management² controls for all software and document changes as follows: (1) the duties for the administration of HUD's configuration management tools are not properly segregated, (2) HUD's contractors do not adequately support its configuration management function, (3) HUD's configuration management documentation is outdated, and (4) a Windows-based HUD application system's change control process was inaccurately executed. These weaknesses exist because not all of the configuration management responsibilities of the HUD information technology services (HITS) contractors who provide information technology infrastructure services are clearly identified. Further, requirements of these performance-based contracts are not defined, which prohibits HUD from effectively evaluating the contractors' performance. Inadequate controls over configuration management could result in unauthorized individuals using system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs.

Duties for the Administration of HUD's Configuration Management Tools Are Not Properly Segregated

The duties for the administration of HUD's configuration management tools are not properly segregated. National Institute of Standards and Technology Special Publication 800-53³ directs organizations to establish divisions of responsibility and separate duties to eliminate conflicts of interest in the responsibilities and duties of individuals. HUD Information Technology Security Policy, Handbook 2400.25, REV-1, applies the principle of least privilege, in which users are granted the most restrictive set of privileges needed to perform authorized tasks and fulfill their job responsibilities and all other privileges are explicitly denied. This ensures that access to sensitive information is granted only to those users with a valid need to know. Below are examples in which duties are not properly segregated:

- A contractor who has been reassigned still has SuperUser access to all client-server applications under the PVCS® configuration management tool. This condition occurred because the "HUD Software Configuration Management Procedures," version 12.1, dated December 2005, does not specify that all PVCS® access requests including SuperUser should be approved by the HUD configuration management director and manager by

² 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.

³ "Recommended Security Controls for Federal Information Systems," dated February 2005.

submitting the proper activation or deactivation form, particularly when there is a change in configuration management supporting personnel. HUD and contractor personnel involved in the configuration management process have accepted the risk associated with this condition. They indicated that it is important to continue this contractor's part-time participation on an as-needed basis to ease the work demands on the configuration management team, which currently supports more than 125 application systems using this tool.

- Five Unix operating system administrators have inappropriate production promotion privilege for the HUD Procurement System, which allows them to access new or changed software releases for this application in PVCS® and to move its releases into the production environment. This privilege is unnecessary since the procurement system is a Windows-based application and, therefore, assistance from Unix operating system administrators to promote new releases to the production environment (i.e., Microsoft Windows servers) is unwarranted. This condition occurred because the production release privilege is granted to all system administrators regardless of the platform being supported.
- The contracted primary system administrators for the configuration management tools on each of the different computer platforms inappropriately also serve as backup system administrators for each other. This gives them the ability to access multiple applications and platforms, thereby increasing the risk of intentional or inadvertent modification of data without authorization. This condition occurred because the contractor cross-trains its personnel with configuration management responsibilities for all configuration management tools.
- Personnel administering PVCS® are also inappropriately involved in the software promotional process, which controls all stages of software changes from the development of source code through implementation into the production environment. Not limiting the promotion process to personnel designated to perform the tasks could result in improper program changes being implemented. This condition occurred because the personnel inappropriately involved in the promotional process do not believe there are a “separation of duties” issue or conflict of interest and reason that the current “working process” minimizes potential discrepancies within PVCS® and implemented production code.

Contractors Do Not Adequately Support the Configuration Management Function

HUD's contractors do not adequately support the configuration management function. For example,

- HUD’s contractors have not provided adequate assistance for installing PVCS® Tracker⁴ and Unix-based TeamStudio⁵ configuration management tools and Windows-based application systems’ production release modules on servers. This condition occurred because the responsibilities for installation of Windows-based applications and the configuration management tools are not clearly defined in the HUD information technology services contracts, service-level agreements, or baseline.⁶
- Insufficient staff is assigned to support the various configuration management tools. For example, there is (1) no resident expert for the configuration management tool for the Unisys platform and (2) only one primary administrator and two backup administrators supporting 128 applications that use PVCS®. In addition, the two backup administrators are not PVCS® subject-matter experts. This condition occurred because the contract service-level agreement does not include sufficient detail for HUD to effectively evaluate the configuration management support provided by the contractors. Also, the performance status report submitted to HUD is the contractors’ self-evaluation, which could be biased and may not be an accurate reflection of the contractors’ performance.

“HUD Configuration Management Procedures” Is Outdated and Ambiguous

The “HUD Configuration Management Procedures” is outdated and unclear. It

- References the Contract Data Requirements List 18 (CDRL 018),⁷ an obsolete document.
- Does not clearly define the responsibilities of both HUD and contractor personnel on the configuration management team.
- Does not clearly define in section 1.3, “CM Policy Correlation,” the responsibilities of the offices that form the Software Development Team. These offices include the Office of System Integration and Efficiency, Real Estate Assessment Center, and Office of Administration.
- Contains a vague description in section 2.1, “CM Policy Roles and Responsibilities,” of roles and responsibilities and fails to identify detailed, specific activities that each office should execute. For example, the Departmental Platforms and Processing Division,

⁴ Tracker is the component that controls and tracks software development activities.

⁵ TeamStudio is the automated configuration management tool for LotusNotes applications.

⁶ The HUD information technology services baseline is HUD’s infrastructure as described in the contract solicitation documents on which the contractors were to prepare their proposals.

⁷ CDRL 018 was a contractor deliverable under the expired HUD Integrated Information Processing Service (HIIPS) contract. It provided procedures for releasing software into the production environment.

Telecomm Processing Division, Customer Service Division, and Systems Integrity and Quality Assurance Division are all responsible for implementing maintenance changes and improvement in software products as directed, approved, and coordinated by the configuration management manager. This gives the appearance that the overall implementation and maintenance responsibilities are shared by four different groups. In reality, each group is responsible for its own area.

This condition occurred because the Office of the Chief Information Officer has undergone a number of reorganizations without clearly defining the roles and responsibilities of each program office and did not identify the roles and responsibilities of two HITS contractors in HUD's Configuration Management Procedures document. According to National Institute of Standards and Technology Special Publication 800-12,⁸ section 2.4, an organization's program policy should assign responsibilities for direct program implementation, and the organization should document a policy with explicit responsibilities.

The HUD Procurement System Configuration Management Plan Is Outdated and Not Officially Approved

The HUD Procurement System configuration management plan, while not officially approved, is outdated and includes obsolete information. It

- Has not been updated since August 2004;
- References the incorrect version number of PVCS's Version Manager,⁹ server name, and location; and
- Does not follow the "HUD Configuration Management Procedures" guidance on obsolete module control.

This condition occurred because, while the application contractor developed the plan, it was not a required contract deliverable. Thus, the contractor is not required to update or prepare it in accordance with HUD's policies and procedures. According to the Government Accountability Office's Federal Information System Control Audit Manual, 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."

⁸ "An Introduction to Computer Security: The National Institute of Standards and Technology Handbook," dated October 1995.

⁹ PVCS® Version Manager organizes, manages, and protects software assets to support software configuration management across an agency's entire enterprise, regardless of platform or development environment.

Administration of the Configuration Management Tool Used for the Procurement System Was Incorrectly Executed

Some of the software modules were not promoted through the correct promotion model stages, and the release version numbers are not unique within the Windows-based HUD Procurement System. National Institute of Standards and Technology Special Publication 800-12, section 9.4.2.3, states that “configuration management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system’s properties, including its security.” We found that

- Software release procedures were not properly followed. Some procurement system modules were not promoted (i.e., moved to the next stage) through the correct stages. For example, the latest release did not promote PowerBuilder¹⁰ source libraries to the final promotion stage called PROD (i.e., production level); several SQL¹¹ modules were inappropriately promoted to DEV (i.e., the development level, which is the first promotion stage) as the final promotion stage; and version labels, which are the critical means of applied version control, for some SQL modules were left blank. These conditions occurred because procedures were not followed.
- The release version numbers recorded in some of the HUD Application Release Tracking System¹² documents for the procurement system are not unique. For instance, document number TC-2004-0482 incorrectly indicated that the release number for both the current and new versions was 3.61. Document number TC-2004-0151 improperly used the same current version number 3.6 and new version number 3.61 as those listed in document number TC-2004-0482. These conditions occurred because the database version numbering scheme is not standardized.

¹⁰ Computer application development system used to draw user interface and reports and access database content.

¹¹ SQL (commonly expanded to Structured Query Language) is the most popular computer language used to create, modify, retrieve, and manipulate data from relational database management systems. The language has evolved beyond its original purpose to support object-relational database management systems.

¹² A database known as “HARTS,” used by HUD to track all software and applications released into the infrastructure.

Conclusion

Absent adequate configuration management controls for software and document changes, HUD increases the risk (1) of destruction or inappropriate disclosure of data and that the reliability of its computerized data will diminish; (2) of damage or disruption of business operations resulting from accidents, errors, or unauthorized use of system resources; (3) that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed; and (4) that outdated policies and plans may not address current risk and, therefore, be deemed ineffective.

Recommendations

We recommend that the Office of the Chief Information Officer

- 1A. Revise the “HUD Configuration Management Procedures” to (1) require submission of activation and deactivation access request forms for PVCS® when there is a change in personnel with configuration management responsibilities, (2) remove all obsolete and inapplicable references, (3) conduct annual reviews and update the procedures to reflect applicable HITS contract modifications and ensure that all designated parties are aware of their roles and responsibilities, and (4) standardize the version numbering scheme used for database change releases.
- 1B. Ensure that PVCS® production promotion privileges are granted only to the system administrators who support the particular platform on which the application resides by following Office of Management and Budget and National Institute of Standards and Technology guidelines pertaining to least privilege and segregation of duties as well as HUD Information Technology Security, Handbook 2400.25, guidance pertaining to granting access on a need-to-know basis.
- 1C. Ensure that EDS provides sufficient and qualified staff as well as adequate training to its staff to perform the structured release process for the application systems that use the PVCS® configuration management tool.
- 1D. Ensure that the HITS 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.
- 1E. Ensure that the contract service-level agreement includes detailed metrics for evaluating contractor-provided configuration management support.
- 1F. Ensure that HUD development teams, test center and database production group personnel properly collaborate and follow all instructions and

procedures included in the configuration management and release documentation.

- 1G. Ensure that test center personnel verify that the version number in the HUD Application Release Tracking System document is unique and that the database production group has confirmed the test center's verification.

We recommend that the Office of the Chief Procurement Officer

- 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.

Finding 2: Access Controls and Support for the IBM Mainframe z/OS Operating System Were Not Adequately Provided

HUD has not ensured that the EDS contractor (1) appropriately implemented security controls over the IBM mainframe operating system console¹³; (2) properly managed the system administer authority on the CA-Top Secret¹⁴ security software; and (3) communicated with HUD information technology management and program offices about IBM operation service disruptions in a timely manner. These conditions exist because HUD has not (1) provided clearly defined guidelines or procedures to the contractors supporting the IBM mainframe operating system and (2) adequately monitored and managed security activities performed by the contractors. As a result, inadequate access controls can diminish HUD's ability to rely on computerized data and increase the risk of destruction or inappropriate disclosure of data.

On January 21, 2005, HUD awarded the HITS contracts to EDS and Lockheed Martin Corporation (Lockheed Martin). The two prime contractors entered into an associate contractor agreement to provide information technology infrastructure services to HUD. EDS operates the data center and help desk and provides disaster recovery. Lockheed Martin provides network and deskside information technology services for HUD headquarters and field offices.

Security Controls over the IBM Mainframe Operating System Console Have Not Been Fully Implemented

Physical and logical access security controls over the IBM mainframe operating system z/OS computer console at the data center maintained by EDS in Charleston, West Virginia, have not been fully implemented. National Institute of Standards and Technology Special Publication 800-12 indicates that physical and environmental protection should be used to protect unauthorized individuals from accessing the media. Logging the use of individual media (e.g., tape cartridge) provides detailed accountability, holding authorized people responsible for their actions. We found that

- Authorized or unauthorized console command entries cannot be traced back to a particular individual. There are more than 70 individuals who are authorized to have physical access to the computer room housing the IBM mainframe operating system consoles. However, not all of them are authorized to make console command entries. Nevertheless, because they have physical access to the consoles, they can enter commands without a logon user ID and password. This condition exists because EDS does not

¹³ The console is a display station from which an operator can control and observe the system operation.

¹⁴ 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.

have a written policy addressing (1) who is authorized to make console command entries and (2) who will oversee and review console command entries.

- After completing the upgrade of the IBM mainframe operating system from OS/390 to z/OS v1.4, EDS did not (1) correctly set console definitions to accurately assign alternate consoles¹⁵ to the main console or (2) remove console and operator access privileges from the temporary consultants who no longer needed access. The alternate console acts as a backup console and is used only to determine why the system console failed. An alternate console cannot be used to install the system. EDS corrected the two conditions after we surfaced the issues.

System Administrator Privileges Are Not Managed Properly

The system administrator privileges under CA-TOP Secret are not managed properly. Improper administrative authority was assigned to some personnel, and the administrative account of a terminated HUD employee was not removed in a timely manner. The CA-Top Secret security software implemented on the IBM mainframe controls and monitors who can access data on the system. However, the access protection exists only if the security features are appropriately implemented. National Institute of Standards and Technology Special Publication 800-53¹⁶ indicates that organizations should grant access based on a valid need to know that is determined by assigned official duties and satisfies all personnel security criteria. Account managers should be notified when users no longer have a valid need to know, and associated accounts should be removed, disabled, or otherwise secured. Account managers should also be notified when users' information system use or need to know changes. Although EDS indicated that the CA-Top Secret administrator reviews users' access privileges daily and the EDS security manager reviews the CA-Top Secret audit report, which shows account additions, deletions, and modifications, we found instances where EDS has not properly managed IBM mainframe accounts.

- MISC9, the most powerful administrative authority, was improperly assigned to HUD employees and contractors who did not have a need for such privileges. One of the privileges MISC9 has is the ability to dynamically change the CA-Top Secret security software parameters. This condition occurred because an information systems security officer responsible for such oversight was not appointed until August 25, 2006. EDS removed the excessive authority from some personnel who did not have a need for the privilege after we surfaced the issue. However, EDS

¹⁵ The alternate console acts as a backup console and is used only to determine why the system console failed. An alternate console cannot be used to install the system.

¹⁶ "Recommended Security Controls for Federal Information Systems," dated February 2005.

did not follow established procedures that require confirmation with HUD management and inadvertently deleted two current HUD employees' IBM mainframe IDs by which users are identified by the security software instead of removing the MISC9 authority. As a result, these two HUD employees are unable to access the IBM mainframe.

- ACID ADP0003, a very powerful CA-Top Secret administrator account that is linked to the master control ID (MSCA) with access to all IBM mainframe resources, was assigned to a HUD employee who had left the department more than a year earlier but was not removed until our inquiry. This condition existed because before September 27, 2006, procedures for deleting accounts that have been inactive for 180 days did not include deleting these types of administrator accounts.
- The ownership, use, and oversight of the CA-Top Secret security software's master security control ID (MSCA) is not defined in any system technical implementation guide or equivalent. This condition occurred because EDS has ownership of the MSCA, and HUD, therefore, is not responsible for developing policies for its oversight.

Service Disruptions Were Not Communicated to the HUD Information Technology Management and Program Offices in a Timely Manner

EDS and HUD information technology management did not communicate disruptions in IBM operation services to the program offices in a timely manner. A major disruption on the IBM mainframe occurred on July 6, 2006, resulting in stoppage of all batch jobs. However, the proper HUD information technology management and program offices were not notified in a timely manner. Also, the recovery process was not appropriately coordinated with the responsible program offices, which could have resulted in damaging applications, including bad application performance, data corruption, and inconsistent data, all of which could lead to the disruption of HUD business functions. EDS claimed that the operational incident notification procedures were already in place but were not properly followed in this instance; however, it did not provide official documentation outlining these procedures. Federal Information Processing Standards Publication 200¹⁷ requires organizations to identify, report, and correct information and information system flaws in a timely manner. In addition, industry standards¹⁸ recommend that procedures be established to handle communication with those affected by or involved with recovery from the incident. The actions to correct system failures should be carefully and formally

¹⁷ "Minimum Security Requirements for Federal Information and Information Systems."

¹⁸ International Standard ISO/IEC 17799, "Information Technology – Security Techniques – Code or Practice for Information Security Management."

controlled so that the integrity of business systems and controls is confirmed with minimal delay.

Conclusion

Without adequate security controls over the operator console, user accounts, and communication among all operational parties, HUD runs the risk that (1) confidential information could be accessible to those who should not see it; (2) unauthorized persons could access, modify, or destroy data, either inadvertently or deliberately; (3) system parameters may be inadequate to prevent unauthorized changes to application programs or data; and (4) incidents may not be handled in a timely manner, possibly damaging applications, which could lead to the disruption of HUD business functions.

Recommendations

We recommend that the Office of the Chief Information Officer

- 2A. Ensure that the necessary internal controls are in place to limit the use of the computer console to those who have a need.
- 2B. Direct EDS to develop and follow written policies establishing (1) who is authorized to make console command entries and (2) who is responsible for overseeing and reviewing console command entries.
- 2C. Ensure that EDS verifies the accuracy of alternate consoles' definitions after each upgrade to the operating system.
- 2D. Ensure that EDS documents the approval of temporary access, automatically terminates temporary and emergency accounts after the completion of assignment, and maintains an accurate list of users with console and operator privileges.
- 2E. Direct EDS to report its daily CA-Top Secret security software administrative tasks to the information systems security officer within the Office of the Chief Information Officer to allow for active and sufficient monitoring. Those tasks should include but not be limited to providing a list of (1) ACIDs and their assigned access privileges and (2) newly assigned and deleted ACIDs.
- 2F. Direct EDS to (1) accurately assign access privileges and continuously monitor ACIDs, (2) oversee the CA-Top Secret security software administrators' tasks, and (3) follow its newly developed administrative ACID review process.
- 2G. Clearly specify the assignment, use, and oversight of the CA-Top Secret Master Security Control ACID (MSCA) in a system technical

implementation guide or equivalent and ensure that EDS complies with the policy.

- 2H. Develop, document, and comply with the official operational incident notification procedures, which should include (1) the technical supporting staff for the program offices that should be included in the notification chain when an operational error occurs, (2) instructions that the HUD operations manager must consult with the technical supporting staff from the program offices so that the HUD operations manager is cognizant of the impact of the incident and can provide guidance to EDS on how to determine the severity level of an incident, and (3) a clear outline of the notification timelines based on the type of incident.

Finding 3: Weaknesses Exist in Physical Security Controls over HUD's Computing Operations Facilities

Physical access to the contractors' data centers and disaster recovery sites is generally restricted to authorized personnel. However, (1) documentation for the network operations center is outdated, (2) established access control procedures at the computer facilities were not followed, and (3) annual shelter-in-place¹⁹ drills were not performed. These conditions exist because the vendors did not comply with federal requirements and their own policies and procedures. Without proper physical access control over computer resources, HUD cannot be assured that its data and resources are protected from intentional or unintentional loss or impairment.

Lockheed Martin manages the network operations center in Maryland, and EDS manages the data center in West Virginia. EDS is also responsible for providing disaster recovery for the data center. While physical access to the centers and disaster recovery sites is generally restricted to authorized personnel, we found some instances in which controls can be improved. These instances occurred because the contractors failed to either review and update documentation for the centers or implement existing procedures.

Documentation for the Network Operations Center Needs To Be Updated

Documentation for the network operations center is outdated. According to the Government Accountability Office's Federal Information System Controls Audit Manual, outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks and, therefore, may be ineffective. We found that

- The physical layout diagram does not reflect the center's current operating functions. The diagram includes outdated references to the tape library and tape vault, which have not existed since the HITS contracts were awarded in January 2005.
- The center's network risk assessment, dated April 2002, is more than three years old and has not been updated to include significant changes made to HUD's information technology and business environment, such as changes resulting from the HITS contract awards.
- The security plan is not current. It identifies the network operations center as the HUD computer center for general support systems and major applications. However, this is contrary to the network operations center's

¹⁹ The goal of sheltering in place during hazardous materials accidents is to minimize the exposure of the threatened public to the dangerous chemical(s). Sheltering in place uses a structure and its indoor atmosphere to temporarily separate people from a hazardous outdoor atmosphere.

function, and the operations of HUD's major application systems were moved to West Virginia.

Established Procedures at Computer Facilities Need to Be Followed

Certain established access controls at computer facilities need to be followed.

- Visitor logs at the network operations center did not include the names of authorized personnel escorting visitors and janitors to the data center and computer room as required by the security plan.
- An EDS employee, whose employment was terminated in October 2005, did not have his access privileges to the computer room in the data center in Charleston, West Virginia, removed until we brought the matter to EDS's attention in August 2006.
- An EDS employee was granted access to the computer room in the data center but was not included on EDS's list of employees authorized to access the facility. In addition, this employee did not have a completed background investigation.

EDS Did Not Perform Annual Shelter-in-Place Drills

Despite West Virginia's Division of Homeland Security and Emergency Management recommendations and EDS security policy requirements that annual shelter-in-place drills be performed, EDS has yet to conduct a shelter-in-place drill. According to the Pollution Information Site scorecard,²⁰ published in 2002, the facility at EDS's data center was ranked 7th of 17 facilities releasing toxic chemicals into the environment. Although a scorecard has not been published since 2002, the most current Toxic Release Inventory²¹ data published by OMB [Office of Management and Budget] Watch,²² last updated in November 2005, indicated that Dow Chemical Company, within the technical center campus on which the data center resides, still produces toxic chemicals. This information further supports the urgent need for an annual shelter-in-place drill.

²⁰ Scorecard: a free public information service founded in 1967 by Environmental Defense and transferred to Green Media Toolshed in November 2005. Scorecard combines data from the U.S. Environmental Protection Agency's Toxics Release Inventory with information on the potential health hazards of toxic chemicals.

²¹ Toxic Release Inventory is a database of information about releases and transfers of toxic chemicals from facilities in certain industrial sectors, including manufacturing, waste handling, mining, and electricity generation. These data match the data used in the Environmental Protection Agency's Toxic Release Inventory Public Data Release documents.

²² OMB [Office of Management and Budget] Watch is a nonprofit research and advocacy organization dedicated to promoting government accountability, citizen participation in public policy decisions, and the use of fiscal and regulatory policy to serve the public interest.

According to the West Virginia Division of Homeland Security and Emergency Management's Web site, accidental chemical spills are more likely to happen than terrorism. As a result, the division requires people living in West Virginia to be prepared to respond to such emergencies. According to EDS, the technical center no longer houses toxic chemicals; therefore, EDS maintains that a shelter-in-place drill is unnecessary. However, the November 2005 Toxic Release Inventory reported data contrary to EDS's claim.

Conclusion

Without adequate physical security controls over HUD's computing environment and resources, such as maintaining current risk assessments, policies, and plans; being adequately prepared for natural disasters or power outages; preventing unauthorized access to computing facilities and resources; and conducting annual shelter-in-place drills, HUD risks that it cannot (1) ensure that all threats, vulnerabilities, and current risks have been identified and addressed; (2) prevent short-term or long-term business disruptions to critical information technology systems, applications, and data; and (3) ensure that access to its computer resources are controlled and protected against unauthorized use, damage, loss, or modifications. Weaknesses in such controls increase the opportunity for unauthorized modification to files and programs and misuse of the computer hardware. Also, absent the performance of annual shelter-in-place drills, HUD cannot ensure that its contractor EDS is prepared to respond to emergencies such as chemical spills.

Recommendations

We recommend that the Office of the Chief Information Officer

- 3A. Ensure that the responsible contractors regularly review and update the facility's risk assessment, physical layout diagram, and security plan to ensure that those documents reflect current conditions of systems and facilities.
- 3B. Ensure that the HITS contractors remove former employees' access privileges immediately upon departure or when the employees' duties no longer require access to computer facilities or resources and ensure that visitor logs for the computer room are filled in completely, including names of escorts.
- 3C. Direct EDS management at the data center in Charleston, West Virginia, to develop, maintain, and test the shelter-in-place plan annually.

Finding 4: Personnel Security Practices Continue to Pose a Risk of Unauthorized Access to HUD Systems

HUD's information technology personnel security practices continue to pose risks of unauthorized access to its systems. Specifically, (1) HUD's Online User Registration System is not fully implemented, (2) HUD has not developed interim reconciliation procedures, (3) quarterly user reconciliations have not been conducted, and (4) contractors have been granted access to sensitive systems without a record of proper background investigations. These conditions exist because HUD cannot efficiently and centrally track and register users at the appropriate access level. As a result, it has no assurance that inappropriate individuals are not being granted access to its information and resources.

For several years, we have reported that HUD's information technology personnel security practices regarding access to critical and sensitive systems were inadequate. The risk of unauthorized access to HUD's critical financial systems remains a major concern. While HUD agreed to our recommendations in this area, they have yet to be fully implemented. The Privacy Act²³ requires agencies to establish appropriate safeguards to ensure the security and confidentiality of records. HUD Personnel Security/Suitability, Handbook 732.3, chapter 4, provides as follows:

- Section 4-10, paragraphs B and C: The Office of the Chief Information Officer is responsible for “. . . In conjunction with program Security Administrators, identifying individuals, HUD employees and contractors, who require background investigations based on their access to sensitive systems. . . . Providing PS [Office of Human Resources Personnel Security] staff with a quarterly list of all individuals who require sensitive access to mission-critical systems within three working days following the end of each fiscal quarter.”
- Section 4-5, paragraph O: The Office of Human Resources personnel security officer is responsible for “. . . Reconciling, as needed, SCATS²⁴ database with the IT [information technology] listing of users who require above query access to mission-critical (sensitive) systems.”

HUD's Online User Registration System Is Not Fully Implemented

In audit report number 2005-DP-0001,²⁵ issued October 19, 2004, the Office of Inspector General (OIG) recommended that HUD develop an action plan to fully

²³ Privacy Act of 1974, Title 5, *United States Code*, Section 552a.

²⁴ Security Control and Tracking System (SCATS) database used by the Office of Security and Emergency Planning to track and monitor background investigations for all HUD employees and contractors.

²⁵ “Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statements Audit.”

implement the HUD Online User Registration System (HOURS)²⁶ to ensure that all user data are tracked and require systems administrators to register users and their access level in this database. The Office of the Chief Information Officer provided OIG with an action plan with a targeted implementation date of May 30, 2005, and the recommendation was closed. However, the system has not been fully implemented. This condition occurred because, while HUD initially elected to use the system to track users' access privileges, the issuance of the HITS contract and ensuing legal difficulties delayed its planned implementation. Later, HUD decided to replace it with another system targeted for implementation by December 31, 2006. Meanwhile, HUD cannot efficiently and centrally track and register users at the appropriate access level.

HUD Has Not Developed Interim Procedures for the Reconciliation Process

In audit report number 2005-DP-0001, OIG recommended that HUD develop interim procedures to identify and link user application access data that can be matched with background investigation data in the Security Control and Tracking System (SCATS) database. This is known as the reconciliation²⁷ process. This recommendation was closed, but HUD did not develop adequate interim procedures. The procedures that HUD developed addressed HUD-wide security controls but did not provide specific instructions to facilitate the reconciliation process. In addition, the Office of the Chief Information Officer indicated that it did not have the capability to track all users for the reconciliation. Full implementation of the HUD Online User Registration System would have enabled HUD to identify all users and reconcile them with the SCATS database. Therefore, until HUD implements a system that centrally tracks all users' access or interim procedures (i.e., specific instructions to facilitate the reconciliation process) that would provide a means to identify all users and match them with the SCATS database, HUD cannot be assured that unauthorized users do not have access to its sensitive systems.

Quarterly User Reconciliations Have Not Been Conducted

The personnel security officer has not performed quarterly reconciliations of users with above-read (query) access to HUD's mission-critical and sensitive systems to the Security Control and Tracking System database. The most recent

²⁶ HOURS is an online registration system that if fully implemented, would contain information about authorized users, including requests for access to automated resources and approvals.

²⁷ The reconciliation procedures were supposed to identify users who potentially have inappropriate access that would not have ordinarily been identified by the usual user's access request process. However, the process was flawed because it did not account for users granted above-read access at the application level.

reconciliation was performed in August 2006; however, before that date, a reconciliation had not been conducted since December 2005. This condition occurred because the EDS contractor employed by the Office of the Chief Information Officer did not provide the personnel security officer the list of users with above-read access in a compatible data format for quarterly data reconciliation. Also, because of limited resources, the personnel security officer did not assign staff to resolve the issue. The Office of Security and Emergency Planning plans to review the current procedures and establish new procedures to train staff.

Contractors Were Inappropriately Granted Access to Sensitive Systems

Contractors, without a record of a proper background investigation, were granted greater-than-read access to sensitive systems. For example,

- Two help desk users, who have access to all general support systems to perform sensitive tasks such as changing user passwords, do not have a record indicating that a background investigation was initiated or completed.
- One system administrator was granted access to sensitive systems but had not had the required background investigation and had not furnished the investigative forms needed for that investigation.
- Two system administrators had background investigations appropriate for the least sensitive position with read-only access.

This condition occurred because the contractors' original access request was for read only. Their access was later upgraded to greater-than-read without HUD going through the proper procedures.

Conclusion

Without adequate personnel security practices, inappropriate users may be granted access to HUD's information and resources, which could result in destruction or compromise of critical and sensitive data. Since user access and the personnel security component currently rely on manual procedures, security is only effective if the procedures are followed because there are no automated controls to enforce them. HUD's information technology personnel security practices continue to pose a risk, and HUD cannot be sure that unauthorized users are not granted above-read access.

Recommendations

We recommend that the Office of the Chief Information Officer

- 4A. Direct EDS to provide the Office of Security and Emergency Planning a list of users with greater-than-read access to HUD's sensitive systems in the requested data format on a quarterly basis.
- 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.

We recommend that the Office of Security and Emergency Planning

- 4C. Perform quarterly reconciliations of the SCATS data with the listing of users with greater-than-read (query) access to sensitive systems to ensure that users either have had adequate background investigations or have furnished required investigative forms matched with their supporting job functions.
- 4D. Assign and train staff to support personnel security functions such as reconciliation of greater-than-read access user data and maintenance and support of SCATS.

SCOPE AND METHODOLOGY

We performed the audit

- From October 2005 through September 2006;
- At HUD headquarters in Washington, DC; the data center in Lanham, Maryland; the data center in West Virginia; the SunGard disaster recovery facilities in Pennsylvania; and the e-mail failover site in Florida; and
- In accordance with generally accepted government auditing standards.

Our review was based on the Government Accountability Office “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. 2006-DP-0005, “Review of HUD’s Information Technology Contingency Planning,” issued August 31, 2006.
- Audit Report No. 2007-DP-0001, “Review of HUD’s Firewalls,” issued October 11, 2006.
- “Review of HUD’s Fiscal Year 2006 Information Security Program,” a draft audit report to be issued February 21, 2007.

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 Hitachi mainframe and Unisys operating system,
- 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 sufficient system software controls over the Windows-based applications (finding 1).
- 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 2, 3, and 4).

FOLLOW-UP ON PRIOR AUDITS

The following recommendations from prior year audits remain open:

**Fiscal Year 2004 Review of Information
Systems Controls in Support of the
Financial Statements Audit: 2005-DP-0001**


- 5C. We recommend that the Assistant Secretary for Administration/Chief Information Officer ensure that risk assessments and business impact analyses are completed on each system.

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

	<p>U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, DC 20410-3000</p>	<i>Hanh DO</i>
CHIEF INFORMATION OFFICER	January 12, 2007	
MEMORANDUM FOR:	Hanh Do, Director, Information System Audit Division, GAA	
FROM:	Lisa Schlessor, Chief Information Officer <i>[Signature]</i>	
SUBJECT:	Comments to the Draft Audit Report on the Fiscal Year 2006 Review of Information Systems Controls in Support of the Financial Statements Audit	
<p>This memorandum is in response to your January 4, 2007, draft audit report on the Fiscal Year 2006 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.</p> <p>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 Donna Eden, Audit Liaison Officer, at ext. 8063.</p> <p>Attachment</p>		

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

Detailed Comments on the Fiscal Year 2006 Review of Information Systems Controls in Support of the Financial Statements Audit

Comment 1

Comment 2

Comment 3

Comment 4

Comment 5

Comment 6

Draft Report Reference	Office of the Chief Information Officer (OCIO) and Management Comments for OIG's Consideration
2007-DP-XXXX	
Page 10 1B, 1C & 1D	<p>OCIO requests the consolidation of recommendations 1B, 1C and 1D. All three recommendations arise from the same issue of least-privilege. The most precise statement concerning this issue is presented in recommendation 1C:</p> <p>Ensure that PVCS production promotion privileges are granted only to the system administrators who support the particular platform on which the application resides.</p> <p>The following suggestion should be added to recommendation 1C: "following the guidelines pertaining to least privilege and segregation of duties." The other two recommendations, 1B and 1D, should be removed.</p>
Page 11 1H, & 1J	<p>OCIO requests the consolidation of recommendations 1H, and 1J. Both recommendations arise from the same issue of ensuring that all instructions and procedures are properly collaborated and followed. Below is a more concise statement combining recommendations 1H & 1J:</p> <p>Ensure that HUD development teams, test center, and database production group personnel properly collaborate and follow all instructions and procedures included in the configuration management, and release documentation.</p>
Page 15 Rec. 2A	<p>OCIO does not concur with Recommendation 2A: Ensure that the necessary internal controls are in place to limit the use of the computer console to those who have a need.</p> <p>These controls are already in place. They are documented in EDS' compliant work instructions. Therefore, we are requesting that this recommendation be removed from the report.</p>
Page 15 Rec. 2B	<p>OCIO does not concur with Recommendation 2B: Direct EDS to develop and follow written policies establishing (1) who is authorized to make console command entries and (2) who is responsible for overseeing and reviewing console command entries.</p> <p>EDS already has these policies in place. They are documented in EDS' compliant work instructions. Therefore, we are requesting that this recommendation be removed from the report.</p>
Page 15 Rec. 2C	<p>OCIO does not concur with Recommendation 2C: Ensure that EDS verifies the accuracy of alternate consoles' definitions after each upgrade to the operating system.</p> <p>EDS has included this step in their work instructions for future system upgrades. Therefore, we are requesting that this recommendation be removed from the report.</p>
Page 15 Rec. 2E	<p>OCIO does not concur with recommendation 2E: Direct EDS to report its daily CA-Top Secret security software administrative tasks to the information systems security officer with the OCIO to allow for active and sufficient monitoring. Those tasks should include but not be limited to providing a list of (1) ACIDs and their assigned access privileges and (2) newly assigned and deleted ACIDs.</p>

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

Comment 7

Comment 8

Comment 9

Comment 10


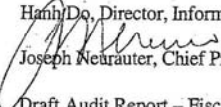
Draft Report Reference	Office of the Chief Information Officer (OCIO) and Management Comments for OIG's Consideration
	<p>Adequate HUD management and technical staff already reviews each access change to CA-Top Secret ACID's. Adding another layer of review would be redundant and without merit. Using the CISO staff for this task will divert resources from the ongoing efforts to conduct Certification and Accreditation and the in-depth training and workshops, which are critical to maintaining green on the PMA scorecard. We would in fact be diverting staff from big ticket, high visibility security items to monitor staff who already have both System Owner approval and HUD management approval to access HUD systems. System Owners should employ reviews of ACID activity for their systems on a regular basis, which would achieve "adequate security controls over...operational parties" within a reasonable scope of work. As background, the IBM mainframe supports an unknown number of users with the CA-Top Secret software. Many HUD systems do not control access to sensitive data through CA-TOP Secret alone. There is an additional layer of access controls and privileges administered through the Program Office staff. Therefore, it is the Program Offices who should be reviewing ACID activity, if any improvements should be made.</p>
Page 15 Rec. 2D	<p>OCIO does not concur with Recommendation 2D: Ensure that EDS documents the approval of temporary access, automatically terminates temporary and emergency accounts after the completion of assignment, and maintains an accurate list of users with console and operator privileges.</p> <p>EDS already has documented and provided to HUD the instructions for the use and management of emergency temporary accounts. Therefore, we are requesting that this recommendation be removed from the report.</p>
Page 16 Rec. 2H	<p>OCIO does not concur with Recommendation 2H: Develop, document, and comply with the official operational incident notification procedures, which should include (1) the technical supporting staff for the program offices that should be included in the notification chain when an operational error occurs, (2) instructions that the HUD operations manager must consult with the technical supporting staff from the program offices so that the HUD operations manager is cognizant of the impact of the incident and can provide guidance to EDS on how to determine the severity level of an incident, and (3) a clear outline of the notification timelines based on the type of incident.</p> <p>EDS has already developed and provided its incident response and escalation procedures, including timeframe for reporting. Therefore, we are requesting that this recommendation be removed from the report.</p>
Page 17 Title Box	<p>OCIO requests the title box of the first section under Finding 3 be changed to read: "Documentation for the Network Operations Center <i>Needs to be Updated.</i>"</p>
Page 19 Rec. 3B	<p>OCIO does not concur with Recommendation 3B: Ensure that the HITS contractors remove former employees' access privileges immediately upon departure or when the employees' duties no longer require access to computer facilities or resources and ensure that visitor logs for the computer room are filled in completely, including names of escorts.</p> <p>This process is already in place. Therefore, we are requesting that this recommendation be removed from the report.</p>

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

 U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, D.C. 20410-3000 OFFICE OF THE CHIEF PROCUREMENT OFFICER	JAN 17 2007
MEMORANDUM FOR:	Hanh Do, Director, Information Systems Audit Division, GAA
FROM:	 Joseph Neurauter, Chief Procurement Officer, N
SUBJECT:	Draft Audit Report – Fiscal Year 2006 Review of Information Systems Controls in Support of the Financial Statements Audit
<p>This memorandum is in response to your January 4, 2007 draft audit report entitled, "Fiscal Year 2006 Review of Information Systems Controls in Support of the Financial Statements Audit." As you are aware, Office of the Chief Procurement Officer (OCPO) staff met with your staff, either in person or via teleconference, on several occasions to discuss the contents of the draft report. In general, the OCPO agrees with the Inspector General findings and recommendations except as noted in the attached comments.</p> <p>We thank you for the opportunity to review the draft report and provide clarification where it is needed. We are looking forward to seeing our comments included in the final report and working with you and your staff to resolve and close out the recommendations. Should you have any questions or need additional information, please do not hesitate to contact Ms. Linda Hooks, OCPO Audit Liaison Officer, at extension 5474.</p>	
Attachment	

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments


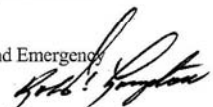
	2								
	<p>Attachment</p> <p>OIG Draft Audit Report</p> <p>FY06 Review of Information Systems Controls in Support of the Financial Statements Audit</p> <p>Ref: OIG Memo dated 1/4/07</p>								
	<table border="1"> <thead> <tr> <th style="text-align: left;">Report Page Reference</th> <th style="text-align: left;">OCPO Comments to OIG Recommendations</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top;"> <p>Comment 11</p> <p>Page 11</p> </td> <td> <p>Recommendation 1K: Annually update the HUD Procurement System (HPS) 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's official's approval of the document to ensure that it is in accordance with HUD's department wide configuration management policies and procedures.</p> <p><u>OCPO Comment:</u></p> <p>Ref 1 & 2) OCPO issued a software development and a maintenance support services contract in December 2006 that includes a requirement to update HPS system documentation and specifically requires update of the Configuration Management Plan to ensure that the plan complies with all HUD documentation standards, policies and procedures. The changes are anticipated for completion not later than May 2008.</p> <p>Ref 3) OCPO is designating a manager to assume responsibility for ensuring OCPO complies with all computer security requirements and other regulatory mandates. This manager will be responsible for reviewing, approving and communicating plan revisions to OCPO employees as appropriate.</p> </td> </tr> <tr> <td style="vertical-align: top;"> <p>Comment 12</p> <p>Page 11</p> </td> <td> <p>Recommendation 1L: Ensure that all procurement system new releases are provided the proper and correct HUD Application Release Tracking System instructions and release version number.</p> <p><u>OCPO Comment:</u> The OCPO designated manager will ensure that future releases reflect the correct release version numbers.</p> </td> </tr> <tr> <td style="vertical-align: top;"> <p>Comment 13</p> <p>Page 11</p> </td> <td> <p>Recommendation 1M: Ensure that all procurement systems' modules have been promoted properly by following PVCS promotion procedures outlined in the "HUD Configuration Management Procedures" document.</p> <p><u>OCPO Comment:</u> OCPO worked with the Configuration Management Team and completed this effort in December 2006 to ensure that all procurement system modules were properly promoted in accordance with HUD configuration management procedures. Additionally, obsolete folders were created for modules that are no longer used.</p> </td> </tr> </tbody> </table>	Report Page Reference	OCPO Comments to OIG Recommendations	<p>Comment 11</p> <p>Page 11</p>	<p>Recommendation 1K: Annually update the HUD Procurement System (HPS) 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's official's approval of the document to ensure that it is in accordance with HUD's department wide configuration management policies and procedures.</p> <p><u>OCPO Comment:</u></p> <p>Ref 1 & 2) OCPO issued a software development and a maintenance support services contract in December 2006 that includes a requirement to update HPS system documentation and specifically requires update of the Configuration Management Plan to ensure that the plan complies with all HUD documentation standards, policies and procedures. The changes are anticipated for completion not later than May 2008.</p> <p>Ref 3) OCPO is designating a manager to assume responsibility for ensuring OCPO complies with all computer security requirements and other regulatory mandates. This manager will be responsible for reviewing, approving and communicating plan revisions to OCPO employees as appropriate.</p>	<p>Comment 12</p> <p>Page 11</p>	<p>Recommendation 1L: Ensure that all procurement system new releases are provided the proper and correct HUD Application Release Tracking System instructions and release version number.</p> <p><u>OCPO Comment:</u> The OCPO designated manager will ensure that future releases reflect the correct release version numbers.</p>	<p>Comment 13</p> <p>Page 11</p>	<p>Recommendation 1M: Ensure that all procurement systems' modules have been promoted properly by following PVCS promotion procedures outlined in the "HUD Configuration Management Procedures" document.</p> <p><u>OCPO Comment:</u> OCPO worked with the Configuration Management Team and completed this effort in December 2006 to ensure that all procurement system modules were properly promoted in accordance with HUD configuration management procedures. Additionally, obsolete folders were created for modules that are no longer used.</p>
Report Page Reference	OCPO Comments to OIG Recommendations								
<p>Comment 11</p> <p>Page 11</p>	<p>Recommendation 1K: Annually update the HUD Procurement System (HPS) 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's official's approval of the document to ensure that it is in accordance with HUD's department wide configuration management policies and procedures.</p> <p><u>OCPO Comment:</u></p> <p>Ref 1 & 2) OCPO issued a software development and a maintenance support services contract in December 2006 that includes a requirement to update HPS system documentation and specifically requires update of the Configuration Management Plan to ensure that the plan complies with all HUD documentation standards, policies and procedures. The changes are anticipated for completion not later than May 2008.</p> <p>Ref 3) OCPO is designating a manager to assume responsibility for ensuring OCPO complies with all computer security requirements and other regulatory mandates. This manager will be responsible for reviewing, approving and communicating plan revisions to OCPO employees as appropriate.</p>								
<p>Comment 12</p> <p>Page 11</p>	<p>Recommendation 1L: Ensure that all procurement system new releases are provided the proper and correct HUD Application Release Tracking System instructions and release version number.</p> <p><u>OCPO Comment:</u> The OCPO designated manager will ensure that future releases reflect the correct release version numbers.</p>								
<p>Comment 13</p> <p>Page 11</p>	<p>Recommendation 1M: Ensure that all procurement systems' modules have been promoted properly by following PVCS promotion procedures outlined in the "HUD Configuration Management Procedures" document.</p> <p><u>OCPO Comment:</u> OCPO worked with the Configuration Management Team and completed this effort in December 2006 to ensure that all procurement system modules were properly promoted in accordance with HUD configuration management procedures. Additionally, obsolete folders were created for modules that are no longer used.</p>								

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

	<p>U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT WASHINGTON, DC 20416-3007</p> <p>2007 JAN 24 PM 3: 54</p>
OFFICE OF ADMINISTRATION	
MEMORANDUM FOR:	Hanh Do, Assistant Director for Information Systems Audit Division, GAA
FROM:	Robert Langston, Director, Office of Security and Emergency Planning, AGE 
SUBJECT:	Comments to the Draft Audit Report on the Fiscal Year 2006 Review of Information Systems Controls in Support of the Financial Statements Audit.
<p>This memorandum is in response to your January 4, 2007, draft audit report on Fiscal Year 2006 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 document.</p> <p>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 Jeff Simpkins, Audit Liaison Officer, at ext. 7180.</p>	
Attachment	
<p>www.hud.gov espanol.hud.gov</p>	

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

Comment 14

Comment 15

Following are OSEP's comments:

OSEP/OCIO is very close to implementation of the new HSPD-12 Personal Identity Verification Process System.

OSEP's new Identity Management System (IDMS) in conjunction with OCIO's new Centralized HUD Account Management Process System (CHAMPS) will ensure that no user is granted access to any system without the proper approvals. The IDMS is a rolls based application that controls the registration process for new employees and contractors beginning with a HUD sponsorship roll, personal identity verification, FBI fingerprint and arrest records check, background investigation, and finally, badge/credential issuance.

CHAMPS is also a rolls based system that ensures no user is provided access to a HUD system without the necessary approvals and background investigations. The ADP Security staff will not grant user access to any HUD system requiring a background investigation without OSEP Personnel Security staff authorizing the request. The ADP Security staff will also not grant basic user access to a HUD LAN without confirmation from OSEP that the user(s) has been properly processed in the OSEP IDMS.

Quarterly Reconciliations

OSEP and OCIO have fine tuned the details on the file format received from EDS on a quarterly basis. The new excel file format simplifies the reconciliation with the SCATS database which is a access data file.

OSEP has been conducting quarterly reconciliations with OCIO since June of 2006.

If and when OSEP has been authorized to hire additional staff, they will be trained on the process.

²⁸ The email headers and related addresses were removed from the auditee's comments.

OIG Evaluation of Auditee Comments

- Comment 1** OIG agrees with the auditee's comment. Recommendations 1B, 1C and 1D have been consolidated as recommendation 1B.
- Comment 2** OIG agrees with the auditee's comment. Recommendations 1H and 1J have been consolidated as recommendation 1F.
- Comment 3** OIG disagrees with the auditee's comment and cannot remove this recommendation from the report. We observed during the audit that physical access to the computer console was not limited to only those who have a need to enter commands on the IBM console. In addition, OCIO did not provide the referenced EDS work instructions for us to evaluate to determine whether the controls are in place as stated.
- Comment 4** OIG has included this recommendation in the final report because OCIO did not provide the referenced EDS work instructions. Upon receipt, we will evaluate this documentation and determine whether the controls are in place as stated.
- Comment 5** OIG has included this recommendation in the final report because OCIO did not provide the referenced EDS work instructions. Upon receipt, we will evaluate this documentation and determine whether the controls are in place as stated.
- Comment 6** OIG disagrees with the auditee's comment. OCIO had concurred with this recommendation as it was initially presented in the notification of findings and recommendations document during the audit. Although OCIO states that adequate HUD management and technical staff already reviews each access change to CA-Top Secret ACIDs, we were not provided with supporting documentation confirming this and therefore, cannot verify whether this control is in place. In addition, we recommended that the information systems security officer (ISSO) within OCIO, not the chief information security officer (CISO) of supporting vendor, performs active and sufficient monitoring of CA-Top Secret administrative tasks. In an e-mail dated September 13, 2006, the CISO confirmed that, as of August 25, 2006, this function was under the ISSO as appointed by the chief information officer.

Finally, Office of Management and Budget Memorandum M-06-20, states that "Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems." Therefore, we disagree with OCIO's statement that "adding another layer of review would be redundant and without merit" and it would be "diverting staff from big ticket, high visibility security items." We also disagree with OCIO's statement that "it is the Program Offices who should be reviewing ACID activity,

if any improvements should be made” because the Program Offices do not possess any CA-Top Secret administrative privileges that would allow them to conduct CA-Top Secret functions such as creating/adding/deleting ACIDs or restricting their application’s data set access.

- Comment 7** OIG has included this recommendation in the final report because OCIO did not provide the referenced EDS work instructions. Upon receipt, we will evaluate this documentation and determine whether the controls are in place as stated.
- Comment 8** OIG has included this recommendation in the final report because we have not been provided with the referenced documentation. Upon receipt, we will evaluate this documentation and determine whether this control is in place as stated.
- Comment 9** OIG agrees with the auditee’s comment. The title box of the first section under finding 3 has been changed as suggested.
- Comment 10** OIG has included this recommendation in the final report because we have not been provided with the referenced documentation. Upon receipt, we will evaluate this documentation and determine whether this control is in place as stated.
- Comment 11** OIG commends the Department for taking immediate actions in issuing a software development and a maintenance support services contract in December 2006 for HPS CM Plan updates and designating a manager responsible for ensuring OCPO complies with all computer security requirements. No modifications were made to the finding.
- Comment 12** OIG commends the Department for taking immediate action in designating a manager responsible for ensuring future releases reflect the correct release version numbers. No modifications were made to the finding.
- Comment 13** OIG commends the Department for taking immediate action in working with CM team to ensure that all procurement system modules were properly promoted in accordance with HUD CM procedures as well as created obsolete folders. No modifications were made to the finding.
- Comment 14** OIG commends the Department for taking immediate action in working with OCIO to perform quarterly reconciliations to ensure that all users would have adequate background investigations matched with their supporting job functions. No modifications were made to the findings.
- Comment 15** OIG disagrees with the Department’s statement that “when OSEP has been authorized to hire additional staff, they will be trained on the process.” Current and newly hired staff who support personnel security functions should have the proper training to perform tasks such as quarterly reconciliations and the use of the new process--CHAMP. No modifications were made to the findings.