audit
report

Issue Date:
October 19, 2004

Audit Case Number
2005-DP-0001

TO: Vickers Meadows, Assistant Secretary for Administration/Chief Information Officer, A

Curtis Hagan

FROM: Curtis Hagan, Director of Information Systems Audit Division, GAA

SUBJECT: Fiscal Year 2004 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 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 2004.

What We Found

We found weaknesses and deficiencies in controls. The weaknesses and deficiencies in controls are related to HUD's noncompliance with (i) requirements for internal controls established by the Office of Management and Budget (OMB), (ii) guidance for securing information systems issued by the National Institute of Standards and Technology (NIST), and (iii) HUD's own policies and procedures.

- HUD's entity-wide information security program does not meet the minimum set of controls established by OMB Circular Number A-130, Appendix III, "Security of Federal Automated Information Resources." Further, HUD has not documented and implemented an information security program as specified in section 3544(b) of the Federal Information Security Management Act (FISMA).

- Controls on the IBM-compatible Hitachi and Unisys mainframes and network do not adequately protect data and application programs from potential unauthorized modification, loss, and disclosure.
- HUD's written software change management procedures are not being followed, making HUD vulnerable to the introduction of unauthorized programs and unauthorized changes to application and system software.
- HUD has not followed guidelines issued by the National Institute of Standards and Technology (NIST) for the development and testing of contingency-related plans, making it uncertain that HUD could recover data processing operations in a timely, orderly manner in the event of a disaster or other unexpected interruptions.

What We Recommend

We recommend that the Assistant Secretary for Administration/Chief Information Officer ensure that OMB requirements, FISMA, NIST 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 Assistant Secretary for Administration/Chief Information Officer concurred with all applicable recommendations. Recommendation 5E was concurred with in principle. The Deputy Assistant Chief Financial Officer for Systems concurred with the applicable recommendation. The complete text of the responses, along with our evaluation of the responses, can be found in appendix A.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

The methodology for performing financial statement audits is provided in the "Financial Audit Manual," which was jointly developed by the Government Accountability Office (GAO) and the President's Council on Integrity and Efficiency (PCIE). 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. [emphasis added]

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 Government Accountability Office's "Federal Information System Controls Audit Manual" (FISCAM) 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 systems,[1] 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.

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

[1] A "general support system" or "system" is defined in OMB Circular Number 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: HUD Needs To Improve Its Information System Security Program

HUD's information system security program has not included the minimum set of controls established by OMB Circular Number A-130, Appendix III, nor has it included all of the requirements for an information security program specified in section 3544(b) of the Federal Information Security Management Act (see appendix B for details). HUD has not met the requirements for (1) periodically assessing and managing risks, (2) developing policies and procedures that are based on assessments of risk and that cost-effectively reduce information security risks to an acceptable level, and (3) clearly assigning security responsibilities.

HUD Did Not Meet Requirements for Assessing Risks

Office of Management and Budget (OMB) and Federal Information Security Management Act (FISMA) requirements for periodically assessing risks have not been met.

- Risk assessments for networks, facilities, and information systems are either out of date or have not been completed as required by section 3544(b)(1) of FISMA and by OMB Circular A-130, Appendix III. As of August 2, 2004, a proposal for the acquisition of contractor assistance in developing risk assessments was under review by HUD management.

- At the end of fiscal year 2003, there were no systems with a current (not more than 3 years old) certification and accreditation.[2] HUD has hired a contractor to assist it in having 36 percent of its applications certified by September 30, 2004.

[2] As explained in Appendix III of OMB Circular Number A-130, some agencies perform "certification reviews" of their systems periodically. These formal technical evaluations lead to a management accreditation or "authorization to process." Such certifications (such as those using the methodology in Federal Information System Processing Standards Publication 102, "Guideline for Computer Security Certification and Accreditation") can provide useful information to assist management in authorizing a system. The authorization of a system to process information, granted by a management official, provides an important quality control (some agencies refer to this authorization as accreditation).

HUD Did Not Meet Requirements for Developing Policies and Procedures

OMB and FISMA requirements for developing policies and procedures that are based on assessments of risk and that cost-effectively reduce information security risks to an acceptable level have not been met.

- Security plans for HUD networks, facilities, and information systems are either out of date, have not been completed, or do not meet guidelines published by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004, and SP 800-18, "Guide for Developing Security Plans for Information Technology Systems," dated December 1998.

- Except for an annual network vulnerability scan, there is no annual testing of management, operational, and technical controls as required by FISMA (section 3544(b)(5)).

- Documentation of HUD's information system security program has not been timely. For years, the only documentation had been HUD Handbook 2400.24, REV-2, dated November 10, 1999. This date precedes enactment of both FISMA and its predecessor, the Government Information System Security Act (GISRA). An updated version of the Handbook was drafted in 2003 but was not issued. The scope of Draft HUD Handbook 2400.24, REV-3, "Security Program Policy," refers to a "HUD Security Program Policy" document. This document did not exist until September 30, 2004 when HUD issued Handbook 2400.25, "Computer Security Policy Handbook."

- There are no written procedures that clearly assign incident response duties and responsibilities and outline the procedures for detecting, responding to, and reporting on security incidents. An incident response policy drafted in September 2001 has not been adopted.

- There has been no systematic attempt to establish and document minimally acceptable system configuration requirements as required by FISMA (section 3544(b)(2)(D)(iii)).

HUD Did Not Meet Requirements for Assigning Security Responsibilities

OMB and FISMA requirements for clearly assigning security responsibilities have not been met:

- While HUD has designated a Senior Agency Information Security Officer, this position does not report directly to the Chief Information Officer. The designated Senior Agency Information Security Officer is serving in an acting capacity.

- System owners, information technology security staff, and systems administrators have not been trained in their information system security responsibilities.

- Duties and responsibilities for detecting, responding to, and reporting on security incidents have not been clearly assigned.

These conditions occurred because HUD does not have an organizational structure that facilitates implementation of security requirements in FISMA, OMB Circular A-130, and NIST publications. For example, HUD has not designated a Senior Agency Information Security Officer position, reporting directly to the Chief Information Officer, empowered with the authority and resources needed to establish a comprehensive information system security program. Without an effective information system security program, HUD is not adequately managing and mitigating the risks (1) of the loss of confidentiality, availability, and integrity of data and (2) that it would be unable to resume business operations and recover essential data after a disruption in computer operations.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer

1A. Create a Senior Agency Information Security Officer position, reporting directly to the Chief Information Officer, that is (i) tasked with establishing an information security program that will comply with FISMA, Appendix III of OMB Circular No. A-130, and applicable NIST publications and (ii) empowered with the authority and resources needed to establish the program.

1B. Establish a schedule for timely certification and accreditation of information systems in accordance with (i) OMB Circular A-130, Appendix III, (ii) NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," and (iii) NIST Federal Information System Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems."

1C. Update and/or develop security policies and procedures (i.e., "Information Security Program Policy," Handbook 2400.24, REV 2, and "HUD Software Development Methodology") that implement requirements of FISMA, OMB, and applicable NIST publications.

Finding 2: Controls Over HUD's Computing Environment Need Strengthening

HUD does not comply with computer security guidelines issued by NIST (National Institute of Standards and Technology) and its own internal policies and procedures in the areas of (1) software change controls, (2) designation of personnel as backup to computer administrators, and (3) access to personnel data.

Improvements Needed for Software Change Controls

HUD Configuration Management Policies and Procedures Documents Do Not Clearly Define Roles and Responsibilities

Configuration management[3] roles and responsibilities are not clearly stated in HUD's "Configuration Management Policies" and "Configuration Management Procedures" documents. As provided in section 3.1.1 of NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," and section 2.4 of NIST SP 800-12, "An Introduction to Computer Security: The National Institute of Standards and Technology Handbook," an organization's program policy should assign responsibilities for direct program implementation and the organization should document a policy with explicit responsibilities. Our review found that

- The HUD "Configuration Management Procedures" document indicates that the Departmental Platforms and Processing Division is responsible for implementing, maintaining, training, monitoring, and enforcing configuration management. However, in the "Configuration Management Policies" document, responsibility for implementing, maintaining, and training of configuration management is divided among three other offices: (i) the Office of Systems Integration and Efficiency, (ii) the Office of Information Technology, and (iii) the Office of the Information Technology Software Development Administrator. None of these offices was assigned the tasks of monitoring and enforcing configuration management in the "Configuration Management Policies" document.

[3] 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.

- The HUD "Configuration Management Policies" document does not identify who is responsible for configuration management quality assurance or which office is responsible for ensuring compliance with the Policies.

This condition occurred because these written policies and procedures are neither reviewed nor updated regularly. Although the written procedures indicate that the documents should be reviewed annually, the last update was completed in October 2002 during a planning reorganization, and the roles and responsibilities were not communicated to the offices and individuals.

Without adequate and aligned policies, procedures, and techniques, all programs and program modifications might not be properly authorized, tested, and approved. In addition, access to and distribution of programs might not be carefully controlled. Without proper controls, there is a risk (i) that security features could be inadvertently or deliberately omitted or "turned off" and (ii) that processing irregularities or malicious code might be introduced. Also, organizational strategic direction and resource assignments for implementation cannot be adequately provided.

Lack of Backup Personnel for Endevor, CoolGen, and CMPlus Administrators

HUD has not ensured that personnel are designated as backups to administrators for the Endevor, CoolGen, and CMPlus[4] configuration management tools. The Department could not provide the names of the backup personnel at the Office of Inspector General's (OIG) request. Its response was that under the HUD Integrated Information Processing Service (HIIPS) contract, the vendor is only required to identify primary system administrators by name and does not need to name backups for every position. According to the GAO "Federal Information System Controls Audit Manual" (section SC-1.2), the resources supporting critical operations to be identified include people.

This condition occurred because the Department does not consider personnel who are backups to administrators for the Endeavor, CoolGen, and CMPlus configuration management tools to be "significant personnel."

[4] HUD uses the automated configuration management tools called Endevor and CoolGen on the IBM-compatible Hitachi mainframe and CMPlus on the Unisys mainframe computers. All software changes must go through Endevor, CoolGen, or CMPlus.

Configuration Management Plan for the Single Family Premium Collection Subsystem – Upfront Needs To Be Updated

The Configuration Management Plan for the Single Family Premium Collection Subsystem – Upfront needs to be updated as indicated in HUD's "Configuration Management Best Practices" document. We found that

- Except for re-engineering projects and the archive enhancements, the Plan does not require changes to system requirements and functions to be documented.
- The Plan does not specify emergency fix libraries.
- Although the Subsystem uses CoolGen as one of its configuration management tools, it is not mentioned in the Plan.

This condition occurred because development activity for the Single Family Premium Collection Subsystem – Upfront has been suspended for the last 2 years. The new software services contract is not in place.

As a consequence, if authorization procedures have not been developed or are not followed, an individual might be able to initiate program changes that (i) result in erroneous processing, (ii) weaken access controls, or (iii) result in improper edits being built into the software. There is also increased risk of (i) the introduction of computer viruses, (ii) errors in the software that lead to bad decisions, and (iii) violation of copyright laws.

User Access List for the CoolGen Production Model is Not Properly Maintained for the Single Family Premium Collection Subsystem – Upfront

The user access list to the Production Model within the CoolGen configuration management environment for the Single Family Premium Collection Subsystem – Upfront is not properly maintained as required by HUD Handbook 2400.24, REV-3. Section 2.1.11 of the Handbook states that Government Technical Representatives and Government Technical Monitors shall maintain an accurate list of contractor staff authorized to work on each system or project. We found a contractor who had transferred to another project several years ago but was still on the access list. We notified the Subsystem Government Technical Monitor on April 23, 2004. As a result, three more users who no longer needed access were identified, and all four were removed as of July 15, 2004.

This condition occurred because the Government Technical Monitor did not notify all appropriate parties to delete the users from system and project access lists. Also, HUD does not have a policy that clearly establishes and communicates the assignment of roles, responsibilities, and procedures for notification of configuration management access activation and deactivation.

As a result, employees who have been terminated or transferred to another project, yet continue to have access to critical or sensitive resources, can pose a major threat, especially those individuals who may have left under less than ideal circumstances.

Backup Personnel Needed for the Hitachi Mainframe Security Administrator

HUD Does Not Have a Dedicated Backup for the Security Administrator

HUD does not have a dedicated backup for the security administrator on the Hitachi mainframe. NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook," states that system administrators need to ensure the continuity of their services.

This condition occurred because the individual assigned as the security backup administrator is currently the Acting Chief Information Security Officer. He has many other responsibilities as well and is, therefore, not a feasible candidate for this position. Without a dedicated backup for the security administrator, HUD does not have assurance that security administration on the Hitachi mainframe will continue to be executed in the absence of the primary administrator.

Sensitive Data in the HUD Central Accounting and Program System Has Not Been Properly Controlled

Access to Sensitive Employee Data on the Vendor Name Inquiry Table Is Not Appropriately Controlled

Access to employee data on the vendor name inquiry table (known as the VNAM table) in the HUD Central Accounting and Program System (HUDCAPS) has not been limited. Records about an individual, including name and identifying number (e.g., Social Security number), can be viewed by 407 users of HUDCAPS. We found that 352 of the 407 users (86 percent) do not need to know this information to perform their jobs. Personnel data in this table include employee name, address, and Social Security number, which is used as the vendor code.

This condition occurred because HUD has not segregated corporate data from employee data in the VNAM table, allowing users who only need to view data regarding commercial vendors the ability to also view sensitive personal data. As a result, sensitive personnel data could be inappropriately disclosed and misused by those with access who do not have a business need for the data.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer

2A. Ensure that the Configuration Management Procedures are reviewed and updated annually.

2B. Update the “Configuration Management Policies” and “Configuration Management Procedures” to clearly identify roles and responsibilities and communicate them to the designated parties.

2C. Include in the “Configuration Management Procedures,” protocols for the activation/deactivation of a user’s access to the configuration management tools.

2D. Ensure that all Government Technical Monitors are aware of their responsibility to maintain an accurate list of contractor staff authorized to work on systems or projects.

2E. Assign competent personnel as backups to administrators for the Endeavor, CoolGen, and CMPlus configuration management tools and communicate the expectation that those personnel are “significant personnel.”

2F. Assign a dedicated backup for the security administrator on the Hitachi mainframe.

2G. Ensure that an update of the Single Family Premium Collection Subsystem – Upfront Configuration Management Plan is part of the services contract to be awarded.

We recommend that the Office of the Chief Financial Officer

2H. Segregate the employee and contractor data on the VNAM table by creating a separate view for users who require access only to vendor data.

Finding 3: Improvements Are Needed in HUD's Networked Environment

We found many vulnerabilities in HUD's networked environment. We found that (1) critical patches are not applied in a timely manner, (2) computer infrastructure information is inappropriately revealed to the public through discussion forums and e-mails sent by the server, (3) audit trails are not reviewed or maintained for an adequate period of time in the Unix and Windows environments, (4) protection of HUD's network connection needs improvement, (5) HUD's intrusion detection system did not detect internal attacks, and (6) there are many vulnerabilities in the Unix and Windows systems and machines and in network devices.

Critical Patches Are Not Applied in a Timely Manner

HUD has not applied critical patches to operating systems on 103 of 419 servers (25 percent). This is contrary to guidelines in NIST SP 800-40, "Procedures for Handling Security Patches." The guidelines emphasize that timely response to vulnerabilities is critical and that organizations should have an explicitly documented patching and vulnerability policy, which includes processes and procedures for handling patches. This policy should specify (i) what techniques will be used to monitor for new patches and vulnerabilities, (ii) which personnel will be responsible for such monitoring, (iii) which systems receive patches and which patches are installed first, and (iv) a methodology for testing and safely installing patches. While the Department identified 16 critical patches released by Microsoft, the 10 that require immediate application were not implemented on 103 servers. Notably, 7 of the 16 patches were initially reported more than 6 months ago. Immediate installation of these patches is essential to prevent unauthorized access to HUD systems.

This condition occurred because HUD's Enterprise Patch Management Policy does not clearly identify individuals' roles and responsibilities. It does not include a precise timeline for applying patches.

Without proper and timely patches, HUD is taking unnecessary risks that an attacker could successfully exploit the most severe of these vulnerabilities to take complete control of the affected system(s). An attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

Computer Infrastructure Information Is Inappropriately Revealed to the Public Through Discussion Forums and E-mails Sent by the Server

Contrary to HUD's own internal policies and NIST guidelines, HUD users inappropriately revealed its computer infrastructure information to the public by way of public technical user group discussions and e-mails sent by the server. According to HUD Handbook 2400.1, "Information Resources Management (IRM) Policies," section 7-3.b, users are not authorized to subscribe to external newsgroups, bulletin boards, or other public forums for non-business-related activities. According to NIST SP 800-45, "Guidelines on Electronic Mail Security," mail servers, mail clients, and the network infrastructure that supports them must be protected. We found that HUD users, particularly contractors, disclosed information about HUD's operating system, database, and software in public technical user group discussion forums. Also, the Lotus Notes server that notifies the sender, which could include persons outside HUD, that a virus has been detected in the incoming e-mail uses the server name in its e-mail address. The server name is valuable information that could be used by hackers to try to gain access to HUD systems.

This condition occurred because HUD users are using their HUD e-mail as their userID in public technical user group discussion forums. These forums generally use the individual user's email address as the userID. When HUD users disclose computer infrastructure information during discussions, the public knows that the information is specific to the Department because "HUD" is included in the user's email address. Further, the Department has not provided training specific to the disclosure of computer infrastructure information.

As a result, sensitive computing information such as server name, database, and programming languages used for the application might be revealed and used by hackers to try and gain access to HUD systems.

Audit Trails Are Not Reviewed or Maintained for an Adequate Period of Time in the Unix and Windows Environment

HUD does not maintain event logs (or audit trails) for an adequate period of time in the Unix and Windows environments and does not routinely review them. According to NIST SP 800-14, logs should be maintained and reviewed periodically. Logs to be maintained should include information sufficient to establish what events occurred and who or what caused them.

OIG network penetration testers completed a vulnerability assessment of HUD's network in early May 2004. Approximately 20 days later, we asked for audit logs from seven Unix and seven Windows servers that we determined to be high risk. HUD was able to provide the logs to the Unix servers but not to the Windows servers. The Windows audit log information had been overwritten because the file had become full. In addition, HUD was unaware that OIG testers had gained control of computers and created userIDs with system administrator rights and capabilities on a Unix and a Windows server. The userIDs created by OIG on both servers were removed after we notified the Department of their existence.

This condition occurred because the Office of the Chief Information Officer has not established and communicated clearly assigned responsibilities and procedures for the maintenance and review of audit logs. The Telecommunications Processing Division and the Information Technology Security Branch assumed that the responsibility of enabling, reviewing, and maintaining audit logs and adequate audit trails belonged to the other party. Additionally, audit logs are reviewed only upon request.

Absent audit trails, the Department risks that unauthorized, unusual, or sensitive access activities will not be detected and that appropriate action will not be taken to identify and remedy the control weaknesses that allowed the incidents to occur. Without prompt and appropriate responses to security incidents, unauthorized activity could continue to occur and cause damage to HUD's information and information technology resources. Further, violators will not be deterred from continuing inappropriate access activity, which could cause embarrassment to the Department and result in financial losses and the disclosure of confidential information.

Protection to HUD's Network Connection Needs Improvement

HUD does not sufficiently protect connections to its network. According to NIST SP 800-48, "Wireless Network Security," Federal agencies should develop a security policy, perform a risk assessment, and actively address risks before deploying wireless technologies. Additionally, the GAO "Federal Information System Controls Audit Manual" (section AC-3.2) states that adequate logical access controls should be implemented to control access between telecommunications systems and terminals and to restrict and monitor access to telecommunications hardware or facilities.

In our tests of network security, we found two wireless connections using 128-bit encryption, which can be easily cracked. This condition occurred because the Department did not implement the Cisco LEAP[5] (Lightweight Extensible Authentication Protocol) on its wireless connections. Industry practices indicate that implementing both 128-bit encryption and LEAP provide proven security for wireless networks. Users of LEAP are advised to use a strong password policy in addition to Cisco LEAP.

In our tests of network security, we also found that any computer can be plugged into a HUD Local Area Network (LAN) drop and automatically be assigned an IP (Internet Protocol) address. No attempt is made to verify that the computer is actually a HUD computer (authorized to be on the network) before an IP address is assigned. For example, a visitor to a HUD office (or a HUD employee or contractor) with his or her own laptop computer can simply plug it into any LAN drop in a HUD office and receive an IP address. With the IP address, which is like a temporary telepone number, the computer can find the IP addresses (phone numbers) for other computers on the HUD network and communicate with them. A HUD computer hosting a HUD application may prompt the visitor's computer for a user identification and password before allowing it into the HUD application system. However, if patches (vendor repairs correcting security flaws) to the operating system on the HUD computer have not been kept current, the visitor's computer could exploit a flaw in the operating system to gain control of the entire computer, including the HUD application. The risk of this happening is somewhat low, given that a person must have physical access to the HUD building and a HUD office or conference room with a LAN drop. However, there are a substantial number of HUD offices, employees, and visitors. This condition occurs because HUD does not use software that checks the unique identification number of the computer's Network Interface Card (NIC) or its Media Access Control (MAC) address. Vendor software is available that could verify that the NIC is on an authorized list before an IP address is assigned. If an IP address

[5] The Cisco LEAP (Light Extensible Authentication Protocol) is a password-based authentication algorithm. It ensures mutual authentication using private and public keys (shared secrets), solving man-in-the-middle attacks, sniffing attacks, and active attacks.

were not assigned to an unauthorized computer, there could be no communication between it and HUD computers, and no harm could be done to HUD information systems.

As a result of these conditions, unauthorized users could gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. If entry points and access paths are not identified, they may not be adequately controlled and may be exploited by unauthorized users to bypass existing controls and gain access to sensitive data, programs, or password files.

HUD's Intrusion Detection System Did Not Detect Internal Attacks

HUD's intrusion detection system,[6] used to detect intrusions into HUD's network and systems, did not detect OIG penetration testing activities. We connected standard laptop computers that were not HUD computers to a HUD LAN and, without using a valid HUD userID and password, gained access to HUD servers by using publicly available hacker tools. HUD's intrusion detection tools did not detect the unusually high volume of internal scanning traffic we generated during the test period.

This condition occurred because HUD does not have an enterprise license to install intrusion detection system sensor software on all HUD personal computers and servers.

Without the ability to promptly detect and respond to security incidents, a hacker could gain control of HUD computers and use them for unauthorized purposes. This could result in financial losses and disclosure or loss of sensitive information.

Vulnerabilities in the Configuration of Unix and Windows Operating Systems and Networks

HUD security controls and practices did not provide adequate protection against unauthorized access to HUD's systems. We found a number of vulnerabilities in

[6] An intrusion detection system is defined in Space and Electronic Warfare Lexicon (www.sew-lexicon.com) as "A computer system designed to detect attacks or attack preparations by monitoring either the traffic on a computer network, an application, or operation system activities within a computer."

Unix and Windows operating systems on HUD's networked computers during an OIG network vulnerability assessment. We provided our findings to HUD in a meeting on June 14, 2004. We further discussed our findings and management's proposed corrective actions and concerns during a second meeting on August 3, 2004. On August 6, 2004, we distributed a written report presenting detailed results of our assessment and recommendations for corrective action. Those results are not provided in this audit report.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer

3A. Ensure that all critical patches are applied in a timely manner and that HUD has an official patch management policy that includes a precise timeline for applying patches.

3B. Train users not to disclose computer infrastructure information in public technical user group discussion forums and requiring that users who join public technical user group discussion forums do not use their HUD e-mail address as their userID.

3C. Change the Lotus Notes Virus Notification configuration to either uncheck the "Warning to sender" and "Send message to sender that entire mail message was blocked" boxes so as not to send a virus notification to the sender or select an ID other than the server name for "Notification message return address" when sending a virus notification to the sender.

3D. Ensure that audit trails are reviewed and maintained for an adequate period of time in the Unix and Windows environment by

(i.) Designating an entity responsible for reviewing audit logs for client server environments.

(ii.) Establishing and communicating clearly assigned responsibilities and procedures for the maintenance and review of audit logs for client server environments.

(iii.) Archiving the audit log information and ensuring that audit logs are not overwritten until the information has been archived for client server environments.

3E. Improve the protection to HUD's network connection by

(i.) Implementing a combination of 128-bit encryption and the Cisco LEAP's authentication for its wireless connection.

(ii.) Preventing the assignment of an IP address to a device (e.g., laptop computer) connected to a HUD network until it has been confirmed that the device is on a HUD-authorized list.

3F. Install intrusion detection system software sensors on all servers.

Finding 4: Access Controls for the Unisys 2200 Operating System Need Strengthening

HUD has not implemented sufficient controls over the Unisys 2200 operating system. It has not (1) documented security policies and procedures; (2) maintained, monitored, or reviewed security events such as user activity and audit logs; (3) provided adequate security training; (4) implemented adequate controls that would not allow users to have excessive privileges to functions that bypass security controls; and (5) enabled the Residue Clear system feature.

HUD Does Not Have Documented Security Policies and Procedures for the Unisys 2200 Operating System

HUD does not have documented security policies and procedures for the Unisys 2200 Operating System. This is contrary to guidance in

- "Department of Defense Trusted Computer System Evaluation Criteria," in which systems assigned a security class rating of C2, at a minimum, are required to maintain documentation.

- NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," which states that all aspects of computer support, operations, and security of a system need to be documented, including security policies and procedures, to ensure continuity and consistency.

- The GAO "Standards for Internal Control in the Federal Government" (Green Book), which provides that internal controls, transactions, and other significant events should be clearly documented; managed; maintained; readily available for examination; and appear in management directives, administrative policies, or operating manuals.

Unisys security personnel acknowledged this condition, which occurred because documented security policies and procedures were not developed due to limited staff and resources and because management did not consider it a priority.

Without documented security policies and procedures for the Unisys 2200 operating system, there is increased risk that controls for ensuring a secure environment are not in place. There is also an increased risk that users may circumvent security mechanisms.

Security Events Such as User Activity and Audit Logs Are Not Maintained, Monitored, or Reviewed for the Unisys 2200 Operating System Platform.

The IT Security Operations Division does not maintain, monitor, or review security events such as user activity and audit logs (TIP and Mapper) for the Unisys 2200 operating system. According to NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," organizations should monitor, record, and periodically review audit logs to identify unauthorized use and to ensure that system resources are functioning properly. According to the "Department of Defense Trusted Computer System Evaluation Criteria," audit information must be selectively kept and protected from modification and unauthorized destruction so that actions affecting security can be traced to the responsible party.

The IT Security Operations Division did not maintain, monitor, and/or review security events such as user activity and audit logs for the Unisys 2200 operating system because

- There are no policies and procedures for reviewing and monitoring security events for the Unisys platform,
- There was no training provided to key personnel assigned to monitor Unisys security reports,
- Security reports could not be produced due to technical problems,
- TIP logs are not enabled, and
- No one has been assigned to monitor and review Mapper logs.

Without maintaining, monitoring, and reviewing security events such as user activity and audit logs, the Department risks that unauthorized, unusual, or sensitive access activities will not be detected, and appropriate action will not be taken to identify and remedy the control weaknesses that allowed the violation to occur. Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an entity's resources indefinitely. Further, violators will not be deterred from continuing inappropriate access activity, which could cause embarrassment to the Department and result in financial losses and disclosure of confidential information.

Staff Has Not Been Provided Adequate Security Training

HUD has not provided the appropriate Unisys security training to all personnel responsible for the security of the Unisys 2200 operating system. Five out of seven did not have the required fundamental Unisys security-related training, and no one has been trained on SIMAN.[7] According to OMB Circular A-130, Appendix III, and the Computer Security Act of 1987, Federal agencies must provide appropriate training for users of Federal computer systems that process sensitive information and train personnel in skills appropriate to the management of that information.

NIST SP 800-16, "IT Security Training Requirements - A Role and Performance Based Model," states that Federal agencies and organizations must ensure that each person involved in today's highly networked environment understands his or her roles and responsibilities and is adequately trained to perform them. Additionally, HUD uses the "Defense Information Systems Agency's Unisys Security Technical Implementation Guide" for its implementation of Unisys security. The Guide provides Unisys training profiles based on function and responsibilities specific to the Unisys platform. For example, personnel assigned to the system security function should receive adequate and continuing education in such classes as SIMAN training and Executive Control Language.

Unisys security staff has not been provided adequate training because

- Management has not developed training profiles that outline necessary skills based on function and responsibilities,

- The Office of Information Technology does not have a training and management succession plan to ensure a timely transfer of knowledge, and

- Training is not monitored and documented to ensure that all security staff are adequately trained.

Without sufficient training, there is increased risk of poor decisions by security staff. This can result in system compromises and increase the risk of unintentional disclosure of sensitive information, damage to critical systems or data, and extremely insecure systems. A properly trained and experienced systems security staff is essential to the security of an organization's computer network.

[7] SIMAN is the software that administers security on the Unisys platform.

Users Granted Excessive Privileges to Functions That Bypass Security Controls

Twenty-six users may have been inappropriately granted privileges to functions that bypass security controls within the Unisys operating system. We determined that the privileges were excessive for 17 of the 26 users based on their job functions. We were unable to determine whether the privileges were excessive for the remaining nine because HUD could not provide us with their job functions. One example of a function that bypasses security controls is permission for the user to start runs under any userID identification, including executing the capabilities of a security officer. According to section 7.2.2 of NIST Federal Information Processing Standard 73, "Guidelines for Security of Computer Applications," access to data should be granted with deliberation of each individual's need for such access, rather than according to rank or position or precedent. Further, OMB Circular A-130, Appendix III (section B), states that least privilege, a system security control, is the practice of restricting a user's access or type of access to the minimum necessary to perform his or her job. Additionally, HUD uses the Defense Information Systems Agency's (DISA) Unisys Security Technical Implementation Guide, which outlines profile levels for a particular user based on the user's job function and responsibilities specific to the Unisys platform. This assists security officers in implementing the principle of least privilege.

This condition occurred because policies and procedures to ensure users are granted the least privilege have not been established and communicated.

Without adequate controls to ensure that users are granted only the minimum privileges necessary to perform specific jobs, there is an increased risk of errors, accidents, unauthorized access, data destruction, potential violations of the Privacy Act, and unintentional disclosure of sensitive information.

Residue Clear System Feature Is Disabled

The Unisys systems administrator disabled the Residue Clear system feature (RESDUCL parameter). This feature clears data from previously assigned storage to ensure that residual data are not available to a newly assigned user who may not be authorized to view the data. Enabling the Residue Clear feature would eliminate the risk that a newly assigned or unauthorized user would be able to retrieve deleted data without the owner's consent.

According to the Department of Defense Trusted Computer System Evaluation Criteria, all authorizations to information contained within a storage object shall be revoked before initial assignment, allocation, or reallocation to a subject from the Trusted Computer Base pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject who obtains access to an object that has been released back to the system. According to the Privacy Act of 1974, records containing identification information (e.g., name and Social Security number) are to be protected from unauthorized use and disclosure.

This condition occurred because the Unisys systems administrator assumed that enabling the Residue Clear system feature would degrade the system's performance level. This assumption was based on a Defense Information System Agency evaluation performed at a Department of Defense site. The evaluation concluded that the Residue Clear feature had a large negative impact on the Unisys 2200 operating system when performing batch-predominant workloads, while having minimal impact when performing transaction—TIP predominant workloads. Since the HUD environment and mix of batch and TIP workloads differ from those at the Department of Defense site, the assumption of degraded system performance may not be valid.

The systems administrator assumed that the Defense Information System Agency had issued HUD a "waiver" from having to enable the feature, as a result of the evaluation performed. However, we determined that the request was not a waiver but a Department of Defense interoffice memorandum that only addressed concerns and justification for Department of Defense sites. Further, there are no supporting documents that this request was approved and that it is a "universal" waiver that applies to all sites using the Unisys 2200 operating system.

Without meeting one or more of the security class rating C2 technical requirements, there are increased risks of opening security exposures in the system. If a system does not meet the "object reuse" requirement (resource isolation), it runs the risk of having deleted data retrieved without the owner's consent and allows the newly assigned user the opportunity to retrieve deleted sensitive or confidential data.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer

4A. Develop and document security policies and procedures for system rules that affect security for the Unisys operating system.

4B. Develop and document policies and procedures for maintaining, monitoring, and reviewing security events for the Unisys platform.

4C. Assign and train personnel on monitoring and reviewing TIP and Mapper logs and Unisys security reports.

4D. Develop and produce usable security reports that document security events for the Unisys platform and ensure that audit logs are enabled, maintained, monitored, and reviewed.

4E. Develop training profiles that identify necessary skills and training based on job function and responsibilities specific to the Unisys platform.

4F. Ensure that key personnel responsible for the Unisys operating system are properly trained to effectively perform their job functions and that the training is monitored and documented.

4G. Develop training and management succession plans to ensure timely transitions of skills and knowledge.

4H. Develop and communicate policies and procedures to ensure that users are granted access to special functions and privileges that commensurate with their responsibilities, and remove excessive access privileges of users who do not need them to perform their job functions.

4I. Ensure that residual data are not available to a newly assigned user who may not be authorized to view the data by

(i.) Conducting a performance evaluation on the Residue Clear feature to determine its impact on workload performance.

(ii.) Enabling the Residue Clear feature if the evaluation determines the impact to be minimal or disable the Residue Clear feature and develop compensating controls.

Finding 5: Contingency Planning Is Needed

There is inadequate assurance that HUD would be able to recover information technology operations in a timely and orderly manner in the event of a disruption at its "production" computer center operated by Lockheed Martin. We found that the Information Technology Contingency Plan (1) has not been updated since November 2003, (2) does not include procedures for the restoration of critical information technology resources and data, (3) has not identified the impact of the loss of critical information technology systems and components, (4) has not assessed data to determine its sensitivity and criticality, and (5) has not been adequately tested.

Information Technology Contingency Plan Should be Updated

During fiscal year 2004, there was an increased risk of HUD not being able to recover information technology systems in the event of an emergency or situation that may disrupt operations. The increased risk was due to complexities arising from bid protests and lawsuits over award of the "HUD Information Technology Service" (HITS) contract to Electronic Data Systems Information Service, L.L.C. (EDS) in August 2003. Lockheed Martin, who previously provided information processing services under the "HUD Integrated Information Processing Service" contract, successfully protested award of the contract to EDS. While the HITS contract was rebid, interim arrangements were put into place that prevented either vendor from assuming full responsibility for disaster recovery. EDS established a disaster recovery facility but Lockheed Martin continued to provide "production" operations and kept emergency tapes of backup data at a nearby storage facility. As a result, disaster recovery must now be coordinated between the two vendors and backup tapes must be transported to the EDS disaster recovery facility in the event of a disruption in Lockheed Martin production operations. In addition, HUD continues to rely upon an outdated and incomplete Information Technology Contingency Plan.

An "Interim Disaster Recovery Plan" was implemented on April 15, 2004. This does not represent an Information Technology Contingency Plan. It is essentially a record of the agreed upon procedures to transition from Lockheed Martin to EDS "in the event of a disaster resulting in the complete loss of the HUD Computer Center (HCC)…." It is a plan for implementing the pre-existing HUD Information Technology Contingency Plan while both Lockheed Martin and EDS provide services to HUD.

HUD's Information Technology Contingency Plan has not been updated since November 2003. It does not include

- Procedures for the restoration of critical information technology resources and data. The impact of the loss of critical information technology systems and components has not been identified. Data have not been assessed to determine their sensitivity and criticality. These identifications and assessments are required to establish the most timely and cost-effective order of systems and data restoration after a disruption.

- Upcoming test schedules. There was a very limited test of the Information Technology Contingency Plan in April 2002. On September16, 2004, we were provided with documentation of limited testing of disaster recovery capability at the EDS disaster recovery facility occurring in March and April of 2004. We were not permitted to observe transition and testing activities as they occurred and we have not had sufficient time to review and assess the test documentation. However, the documentation indicates that testing was limited to disability of certain mainframe computer capability while all other resources remain available. This testing was not, nor intended to be, a realistic simulation of a disaster. To our knowledge, recovery from a scenario in which the entire HUD Computer Center is disabled has never been tested. To our knowledge, no other tests are planned.

- A contingency planning policy statement. This statement outlines the Plan's update/maintenance schedule.

NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," indicates that

- The contingency plan must include a strategy to recover and perform system operations at an alternate facility for an extended period.

- Business impact analyses should be completed for each system to establish the sequence of recovery for HUD's systems.

- The Information Technology Contingency Plan should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the plan, system, business processes supported by the system, or resources used for recovery procedures, including a new Disaster Recovery Facility or equipment.

These conditions occurred because management decided not to update or comprehensively test the existing Information Technology Contingency Plan in anticipation of significant changes to the information technology infrastructure and development of a new plan as part of the new contract. Instead, an Interim Disaster Recovery Plan was implemented on April 15, 2004. However, this document does not represent an Information Technology Contingency Plan.

Further, the Contingency Plan coordinator has not completed business impact analyses to determine the priority of restoration for information technology systems. Program area managers have not completed risk assessments to identify and prioritize the restoration of data based on sensitivity and criticality. While HUD has indicated that a business impact analysis was completed in response to an OIG audit recommendation,[8] the Department could not produce a copy for our review.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer ensure that

5A. The "IT Contingency Plan" is updated to reflect current conditions.

5B. The "IT Contingency Plan" is reviewed for accuracy and completeness at least annually.

5C. Risk assessments and business impact analyses are completed on each system.

5D. A recurring "IT Contingency Plan" test schedule is developed and implemented.

5E. HUD store backup production data at the EDS Disaster Recovery Facility.

[8] Recommendation 5a of Audit Report Number 2003-FO-0004, "U.S. Department of Housing and Urban Development Audit of Financial Statements, Fiscal Years 2002 and 2001."

Finding 6: Personnel Security Practices Continue To Pose a Risk of Unauthorized Access to Departmental Systems

Although improvements have been made and corrective actions have been taken to address recommendations in last year's report on the fiscal year 2003 financial statements, we found that additional weaknesses exist in the Department's management of its personnel security function. The Department does not have a central repository that would account for all users with above-read (query) access to all HUD general support and application systems. Consequently, HUD has no assurance that all users who have access to HUD's sensitive systems have had the appropriate background investigation. We found that 75 of approximately 2,800 users who were granted above query access to sensitive application systems may not have had the required background investigation.

HUD Has Not Fully Implemented the Online User Registration System

The Department does not have a central repository that would account for all users with above-read (query) access to all HUD general support and application systems. We previously reported that the Information Technology Operations Security Branch does not track users with above-read access at the application level. That is, while the Security Branch initially granted read access to the user, the systems administrators for the various applications may subsequently upgrade the user's access. Those with above-read access to sensitive application systems are required to have a background investigation. Without a complete list of users with above-read access, the personnel security officer is unable to perform a full reconciliation of these users to the Security Control and Tracking System database that tracks background investigations for all HUD employees and contractors. In addition, the reconciliation process is cumbersome because it is done by name, and the names may not be identical between the Security Control and Tracking System database and the listing provided by the Information Technology Operations Security Branch. We found 75 of approximately 2,800 users who were granted above query access to sensitive application systems may not have had the required background investigation.

HUD Handbook 732.3, "HUD Personnel Security/Suitability," chapter 4, section 4-10, paragraph B, provides that the Office of Chief Information Officer, in conjunction with program security administrators, is responsible for identifying individuals, HUD employees and contractors, who require background investigations based on their access to sensitive systems. Additionally, section 4-10, paragraph C, requires the Office of Chief Information Officer to provide the Office of Human Resources Personnel Security staff with a quarterly list of all individuals who require sensitive access to mission-critical systems within 3 working days following the end of each fiscal quarter. Section 4-5, paragraph O, also provides that the Office of Human Resources Personnel Security Officer is responsible for reconciling, as needed, the Security Control and Tracking System database with the information technology listing of users who require above query access to mission-critical (sensitive) systems.

This condition occurred because HUD has not fully implemented the HUD Online User Registration System. If fully implemented, the System would contain information about authorized users, including requests for access to automated resources and approvals. All systems administrators will be required to register users and their access level into this database when it is fully implemented. HUD has not developed procedures to identify and link user application access data that can be matched with background investigation data in the Security Control and Tracking System**.**

Without ensuring that all users who have access to HUD's sensitive systems have had the appropriate background investigation, there is increased risk that unsuitable users may intentionally misuse, damage, or destroy HUD's data.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer

6A. Develop an action plan to fully implement the HUD Online User Registration System, ensure that all user data are tracked, and require systems administrators to register users and their access level into this database.

6B. 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 database.

SCOPE AND METHODOLOGY

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

- Ensure an adequate, entitywide information security planning and management program;
- 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; 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 the Department to address vulnerabilities identified in our fiscal year 2003 audit.

We performed audit work at the HUD Headquarters in Washington, DC; the Data Center in Lanham, MD; and the Disaster Recovery Facility in West Virginia. The audit covered the period October 2003 through August 2004.

The audit was conducted in accordance with generally accepted government auditing standards and included such tests and other audit procedures that we considered necessary under the circumstances.

Scope Limitation

On March 1, 2002, the Department issued a Request for Proposal to replace the HUD Integrated Information Processing Service (HIIPS) contract with Lockheed Martin that was set to expire in May 2003. Vendor proposals were received during May 2002 for a "HUD Information Technology Service" (HITS) contract. Electronic Data Systems Information Service L.L.C. (EDS) won the competition and was awarded the new HITS contract on August 14, 2003.

The transition of information technology operations from Lockheed Martin to EDS that began in August 2003 created unusual risks in our judgment. Our understanding was that institutional knowledge of HUD systems and applications gained over a period of 10 years had to be transferred from Lockheed Martin personnel to EDS personnel–while Lockheed Martin was winding down operations and Lockheed Martin personnel were finding other employment. EDS had to establish a new data center; acquire and install data processing equipment; install and configure operating systems; hire skilled personnel; subcontract for certain services; develop its policies, procedures, practices, and controls; and quickly gain an understanding of HUD systems and applications. In our judgment, there was much that could go wrong under these circumstances and we therefore perceived an increased risk of loss of the integrity, confidentiality, and availability of HUD's data.

We attempted to assess how the risks we perceived in these unusual circumstances were being controlled and mitigated. We were prevented from doing so by HUD management. For example, HUD would not provide us with a copy of the transition plan developed by EDS. In addition, knowledgeable HUD and Lockheed Martin personnel we attempted to interview told us that they were not permitted to discuss these matters with us. Consequently, the results of our audit are qualified in that we were unable to assess how the risks associated with the transition of information technology operations from Lockheed Martin to EDS were controlled and mitigated.

The transition was not completed. Lockheed Martin filed a bid protest with the Government Accountability Office (GAO) soon after HUD awarded the HITS contract to EDS in August 2003. EDS continued work on the contract while GAO considered the bid protest. In December 2003, GAO upheld Lockheed Martin's protest and recommended that HUD open a new competition for the HITS contract between EDS and Lockheed Martin. HUD agreed and sent letters to EDS and Lockheed Martin on January 30, 2004 informing the contractors that work would be split between them until a new contract was awarded. In early February 2004, Lockheed Martin requested an injunction and temporary restraining order from the U.S. Court of Federal Claims to stop EDS from working on the HITS contract. As a result of court-ordered negotiations, the transition of information technology operations from Lockheed Martin to EDS was suspended in February 2004, six months after initial award of the HITS contract to EDS. EDS continued to provide operations that had been transitioned from Lockheed Martin (i.e., a nationwide help desk, field support service, and a disaster recovery facility). Lockheed Martin continued to provide all other services from its facilities.

After considering new bids from EDS and Lockheed Martin, HUD re-awarded the HITS contract to EDS on August 6, 2004. Shortly thereafter, Lockheed Martin filed three bid protests with the GAO. GAO has scheduled decisions on the bid protests for November 24, 2004, December 8, 2004, and December 17, 2004.

INTERNAL CONTROLS

In planning and performing our audit, we obtained an understanding of the management controls that were relevant to our audit. Management is responsible for establishing effective management controls. Management controls, in the broadest sense, include the plan of organization, methods, and procedures adopted by management to ensure that its goals are met. Management controls include the processes 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:

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

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 its security program met requirements established by the Office of Management and Budget in Circular A-130, Appendix III, and section 3544(b) of the Federal Information Security Management Act (see finding 1).

- During fiscal year 2004, it was unlikely that HUD would have been able to recover information technology operations in a timely and orderly manner in the event of a disruption at its “production” computer center operated by Lockheed Martin (see finding 5).

- HUD did not have a system to ensure sufficient system software controls over the Hitachi mainframe and the Unisys operating system (see findings 2 and 4).

- HUD did not have a system to ensure that controls and practices would protect its critical and sensitive systems and networked environment against unauthorized access (see findings 3 and 6).

FOLLOW-UP ON PRIOR AUDITS

We followed up on recommendations from prior year audits and found that the following remain open:

Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit: 2004-DP-0001

1A Prepare an action plan to ensure that all HUD major applications and general support systems are developed and kept in compliance with requirements set forth by Appendix III of OMB Circular A-130, NIST publications, and HUD's internal standards.

1B Follow NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," by (a) performing certification and accreditation to test and evaluate the technical and non-technical security features of the systems; (b) requiring implementation plans to identify and examine all relevant technical, security, and administrative issues surrounding the interconnection for establishing the interconnection; (c) requiring written system interconnecting agreements, to include an Interconnection Security Agreement and a Memorandum of Understanding (or Agreement); (d) ensuring that written system interconnecting agreements are included in the systems security plans; (e) reviewing security controls for the interconnections at least annually or whenever a significant change occurs to ensure they are operating properly; and (f) analyzing audit logs on a regular basis to detect and track unusual or suspicious activities across the interconnection.

1C Improve access controls to Departmental systems by (a) implementing a bi-annual (at a minimum) userID deletion schedule to remove those userIDs that have been inactive for more than 6 months. A CA-EARL job to verify the userIDs inactive for more than 6 months should be established); b) ensuring that requests to remove departed users' userIDs are carried out and that the requestors are notified of the removal; (c) carrying out procedures to remove resources (datasets) associated with deleted userIDs as well as their "catalog alias" from the mainframe (this includes ensuring that the Information Technology Operations Security Branch initiates the request to the Departmental Platforms and Processing Division, which would notify the Security Branch when the removal is completed); and (d) assigning a competent person, who possesses the required technical skills and is available during core business hours, as a dedicated backup for the Top Secret administrator.

1F Correct the weaknesses identified by the subcontractor's vulnerability assessment.

1G Upgrade to the next release of the InSync Single Sign-On software product, which uses AES, scheduled for release next year.

1H Implement the Windows 2000 password rules recommended by the National Institute of Standards and Technology, National Security Agency, and Microsoft as follows: (a) set the account lockout to three invalid logon attempts, (b) set the password history to 24 passwords, (c) set the minimum password length for non-systems administrators to eight characters, (d) set the minimum password length for systems administrators to greater than 12 characters, if possible, and (e) set the password syntax to require a mix of regular and special characters.

1I Monitor and evaluate configuration management activities (e.g., through quality assurance reviews) to ensure that HUD policies and procedures are followed.

2A Adopt NIST SP 800-34, "Contingency Planning Guide for Information Technology System," for developing contingency-related planning as follows: (a) adopt the seven steps; (b) adopt definitions for the various contingency-related plans; and (c) develop additional plans and revise current plans to address the entire suite of contingency-related plans to include (1) Business Continuity Plan, (2) Business Recovery (or Resumption) Plan, (3) Continuity of Operations Plan, (4) Continuity of Support Plan/Information Technology Contingency Plan, (5) Crisis Communications Plan, (6) Cyber Incident Response Plan, (7) Disaster Recovery Plan, and (8) Occupant Emergency Plan.

2B Ensure that contingency-related plans are updated or developed to take into consideration non-traditional disasters such as massive regional power blackouts like the one that occurred on August 14, 2003, and terrorist strikes of the magnitude of the September 11, 2001, attacks. For example, plan assumptions and scenarios should address scenarios in which more than one facility is affected at the same time, including significant delays with respect to the availability of highways, airports, trains, buses, police, firefighters, rescue workers, and key personnel.

2C Ensure that testing is conducted on contingency-related plans by (a) testing the COOP at the alternate site as outlined by FPC 66, "Test, Training, and Exercise Program for Continuity of Operations"; (b) developing and testing a contingency plan for the transition phase, during which the workload and equipment from the current Disaster Recovery Facility in Virginia and the Data Center in Maryland will be installed and migrated to the new Disaster Recovery Facility in West Virginia; and (c) following NIST SP 800-34, "Contingency Planning Guide for Information Technology System," by first individually testing each element of the contingency plan and then testing it as a whole to confirm the accuracy of recovery procedures and its overall effectiveness. Testing should occur at least annually and when significant changes are made to the information technology system, supported business processes, or the Information Technology Contingency Plan.

Application Control Review of the Tenant Rental Assistance Certification System (TRACS): 2004-DP-0002

1A Enforce current policies requiring system owners, with the assistance of their program supervisors and security administrators, to ensure that system access is based on the need to perform specific job functions.

1C Enforce current policies that require the security administrator, with assistance from the Information Technology Operations Security Branch, to identify individuals having access to TRACS and to conduct quarterly reviews of all userIDs issued to determine whether all users still have a valid need to access resources and data at their current level of privilege.

1F Ensure that the Information Technology Operations Security Branch provides the TRACS security administrator with the appropriate user ACLs.

1G Remove access to data and privileges of users who do not require them to perform their job function.

2A Remove development programmers' greater-than-read access privileges to TRACS production libraries and data files and use discretion to grant temporary greater-than-read access privileges during emergency situation occurrences only.

2B Enforce (1) adherence to the configuration management emergency fix procedures and (2) use of maintenance libraries after developing a job control language that will allow regular updates to the maintenance library.

2C Ensure that the TRACS system owner includes the policies and procedures in the TRACS Configuration Management Plan and inform TRACS contractor support staff about the procedures to ensure optimum synchronization of all production modules with both the Endevor and PVCS modules.

3A Ensure that adequate resources are available for implementation of mandatory and periodic security training for all individuals, including but not limited to the system owner, information systems security officer, and HUD employee and the [TRACS Please write out if possible contractor support staff involved in the management, use, or operation of [TRACS Please write out if possible.

3B In coordination with the Chief Information Officer, establish a Memorandum of Understanding with PHA coordinators that establishes those security-related controls addressed by the HUD Security Program and ensures that TRACS Internet users are provided adequate system security training.

4A Enforce the use and periodic review of the audit logs to detect security violations, performance problems, transactions, and flaws in the application or monitor and log user activities, including data files opened and closed; specific actions, such as reading, editing, and deleting records fields; and printing reports.

5A Enforce adherence to the policy requiring users requesting above-read access to HUD's mission-critical and sensitive systems to submit proper investigation forms before they are allowed access to the systems.

5B Ensure implementation of a central repository that would serve as a master inventory tracking system to track all users' access levels for HUD's general support systems and application systems.

6A. Ensure that the Office of Multi-family Housing has the resources necessary to obtain qualified and knowledgeable staff necessary to support the security functions of the Tenant Rental Assistance Certification System and that technical support responsibilities and security-related tasks are clearly assigned to separate staff members (e.g., segregate the duties of the TRACS security administrator, database administrator, and technical lead) to ensure proper segregation of duties and responsibilities between the (1) development, testing, and production functions within the Endevor environment and (2) TRACS DB2 database administrator, Endevor approver group, and CoolGen administrator.

6B Reduce production access privileges for TRACS development computer programmer(s) to read-only and follow emergency fix procedures when a programmer's intervention is required to resolve production abends.

Public and Indian Housing Information Center (PIC), Public and Indian Housing: 2004-DP-0003

1A Archive the data stored on the Web server to the database after the data are input and accepted by the system.

1B Re-design the alternate identification generator in a way that requires input of the alien registration number, captured in line 3p on the HUD Form 50058, before an alternate ID can be issued.

1C Re-design the PIC system to allow for the creation and use of an alternate ID only in instances in which a Social Security number cannot be provided.

1D Establish controls with the Social Security/alternate ID field that prevent a head of household from obtaining assistance using an alternate ID and a Social Security number.

1E Re-design the PIC system to ensure that adequate controls are placed in the Social Security number field. The Social Security number should continue to be a required field with appropriate controls to validate the number with the exception of when an alternate ID is generated. Controls should be implemented to ensure that Social Security numbers are nine digit numeric and that obviously invalid numbers; i.e., 123-45-6789, are not accepted. The field should contain appropriate controls to validate the alternate ID.

1F Establish controls within PIC to require all household members 6 years of age and older to supply a Social Security number, an alien registration number, or a valid system-generated alternate ID.

1G Establish controls within the system to check for duplicate use of member of household Social Security numbers.

1H Establish validation controls on all Social Security number fields and reject Form HUD 50058 submissions that use invalid Social Security numbers.

1I Establish validation checks to ensure that no head of household is listed as a household member on another unit and that no household member is listed as a head of household.

1J Establish a validation process through the Social Security Administration to ensure that tenant-supplied Social Security numbers are valid.

1K Institute regulations and policies and procedures for the Public Housing Agencies, requiring them to obtain and report to HUD through PIC the Social Security number or applicable immigration status information (i.e., an alien registration number) for all heads of households and family members receiving assistance under programs run by the Office of Public and Indian Housing.

1L Establish policies and procedures that enforce the requirements of 24 CFR Part 5, requiring all household members that can obtain a Social Security number to do so to be eligible for assistance.

1M Establish policies and procedures governing the issuance of alternate ID's within PIC, that limit the creation of these numbers to individuals who are unable to obtain a Social Security number or alien registration number.

2A Establish and implement, with the assistance of applicable program staff, business rules to ensure that obsolete data in the database are identified and archived to the historical database, including obsolete data from the old MTCS system.

2B Initiate a project to track and follow up on noncompliance of annual reexaminations for Public Housing.

2C Determine why the limit check on the total tenant payment field is not functioning properly and make the necessary system corrections to re-establish this control.

2D Reassess the limit check on the total tenant income field in PIC to determine if the field should have a fatal error associated with it.

2E Ensure that the building and unit data inventory in PIC is corrected through a one-time, 100-percent certification of the data in PIC by the Public Housing Agencies and after completion of the correction process, initiate an annual verification strategy, based upon risk, to ensure that building and unit data remain accurate.

2F Establish a mechanism to allow for the correction of building and unit data in PIC once approved within the system.

2G Ensure that a baseline date is established between the demolition and disposition data in IBS and the data in PIC to ensure that HUD has accurate and complete records.

2H Reassess the manner in which the reporting rate is calculated in PIC. Work with the PIH to create a fair measurement of PHA performance that does not use questionable and unreliable data.

3A Establish a document that defines all edit checks and system processing.

3B Establish a quality assurance process to collect 50058 data and building and unit upload data to identify error trends and possible corresponding process improvements.

3C Determine through gap analysis what enhancements or modifications would be required to make the system function properly and provide the functionality that the Department requires before implementing further system enhancements.

Public and Indian Housing Information Center (PIC), Public and Indian Housing: 2003-DP-0001

1A Conduct a comprehensive security review of the PIC system. This review should include conducting sensitivity and risk assessments and formulating comprehensive security policy and goals. This security review should be used to form the basis for developing comprehensive security policies and procedures, security standards, and controls to ensure that PIC system-critical data and resources are adequately safeguarded against waste, fraud, or abuse.

1B Conduct a review of the roles and responsibilities and access rights based on the business rules and the sensitivity of data. From this review, build SQL queries based on the security logic design to establish a process to monitor users' access.

1C Remove the application Security Administration function from the PHA's and the vendors and assign it to HUD personnel only.

1D Establish a comprehensive process for monitoring and validating, on a semi-annual basis, users' access to the PIC system. This recertification process should include developing policies and procedures that include (a) developing access control lists of users (including groups, machines, and processes), (b) how access to the system should be requested and granted and what information should be obtained and maintained on users, (c) limiting access granted to users outside the HUD organization to predefined roles with access levels determined by HUD staff, and (d) specifics regarding who can be assigned security administration rights within the system and how this access will be monitored.

1E Ensure that controls are in place for the creation and assignment of roles in the Security Administration submodule. Additionally, roles in the Security Administration submodule that are not used or are duplicative should be removed. Also, roles should be fully described to determine what they were created for.

1F Perform a review of the roles and responsibilities of PIC users and establish policies and procedures that identify and define global roles within the PIC system that maintain a proper segregation of duties to include (a) ensuring HUD security administrators do not have the ability to submit Form HUD 50058 data and (b) creating separate global system and security administration roles within the PIC organization that divide responsibility for data correction and system security functions.

1G Establish system-specific policies and procedures for maintaining and controlling the confidentiality of user passwords and IDs.

1H Establish policies, procedures, and standards for reviewing audit logs. The audit logs should be reviewed by personnel other than security and/or administration personnel who maintain logical access functions.

1I PIH should ensure that PIC security module and the SQL Server 2000 incorporate the following identification and authentication controls:

- Password length is set to a minimum of eight characters.
- Passwords are set to expire every 60 days or sooner.
- Passwords are required to contain special characters, not be in an online dictionary, and be unrelated to the user ID.
- Passwords are made inactive after three unsuccessful login attempts.
- A history file is established to ensure that previously used passwords are not used again.
- User accounts or IDs that have been inactive over a period of 6 months are disabled. User accounts that are inactive over a period of 12 months should be permanently disabled.
- All users are given individual and distinct user IDs to ensure user accountability.

1J Ensure adequate separation of duties by separating the processes for account setup and authorization so that PIH does not control both functions.

1K. Ensure that the access controls over the SQL Server 2000 are strengthened by using the audit log function capability under the current release version of the SQL Server, to include enabling of the C2 auditing mode feature.

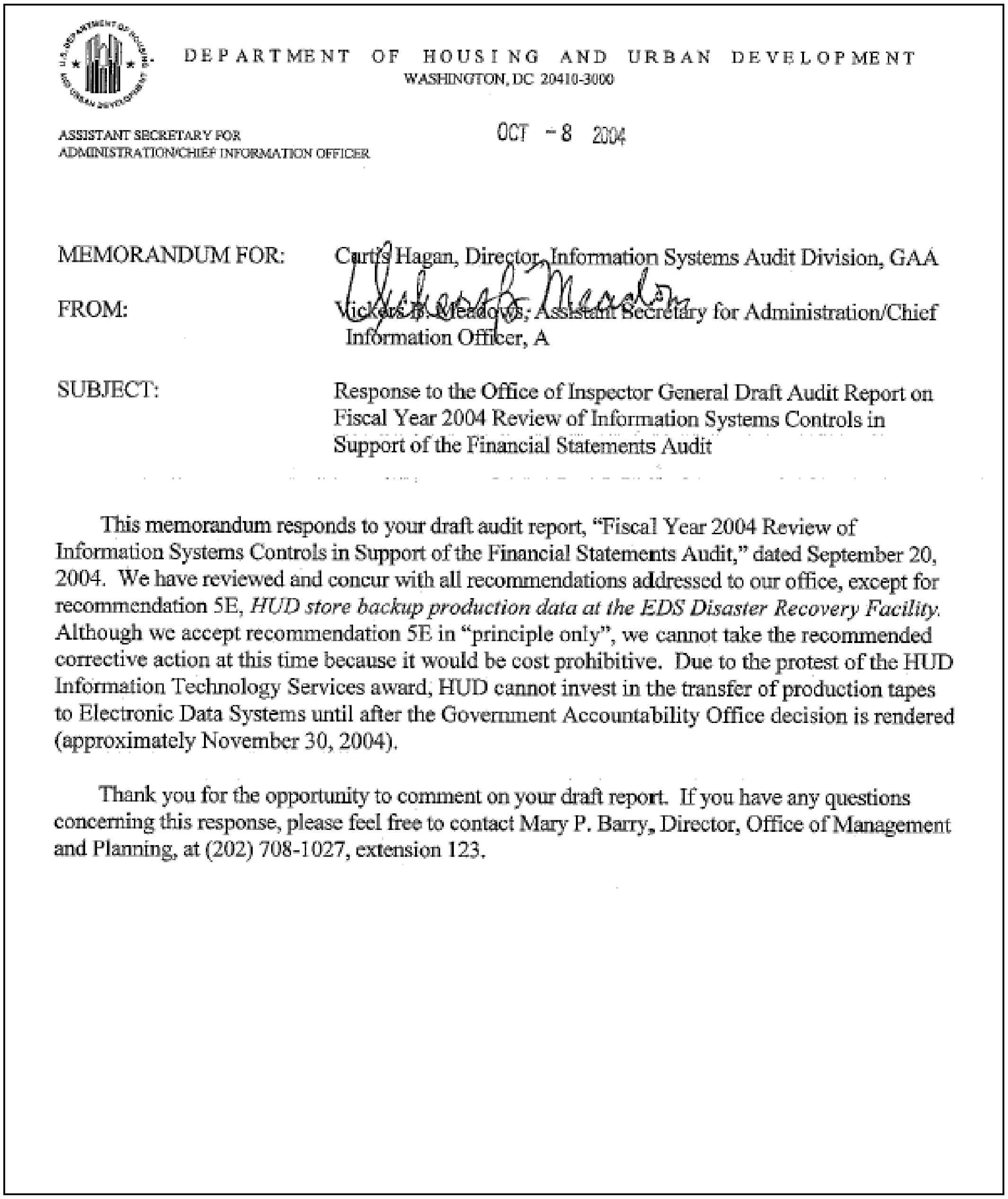
1L. Develop an alternative to SQL Server 2000 security mode, which has weak authentication controls. An alternative would be to use “mixed mode.” Mixed mode combines the SQL Server 2000 and Windows 2000 IDs using the robust access controls of Windows 2000.

APPENDIXES

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation **Auditee Comments**



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

ASSISTANT SECRETARY FOR
ADMINISTRATION/CHIEF INFORMATION OFFICER

OCT - 8 2004

MEMORANDUM FOR: Curtis Hagan, Director, Information Systems Audit Division, GAA

FROM: Vickers B. Meadows, Assistant Secretary for Administration/Chief Information Officer, A

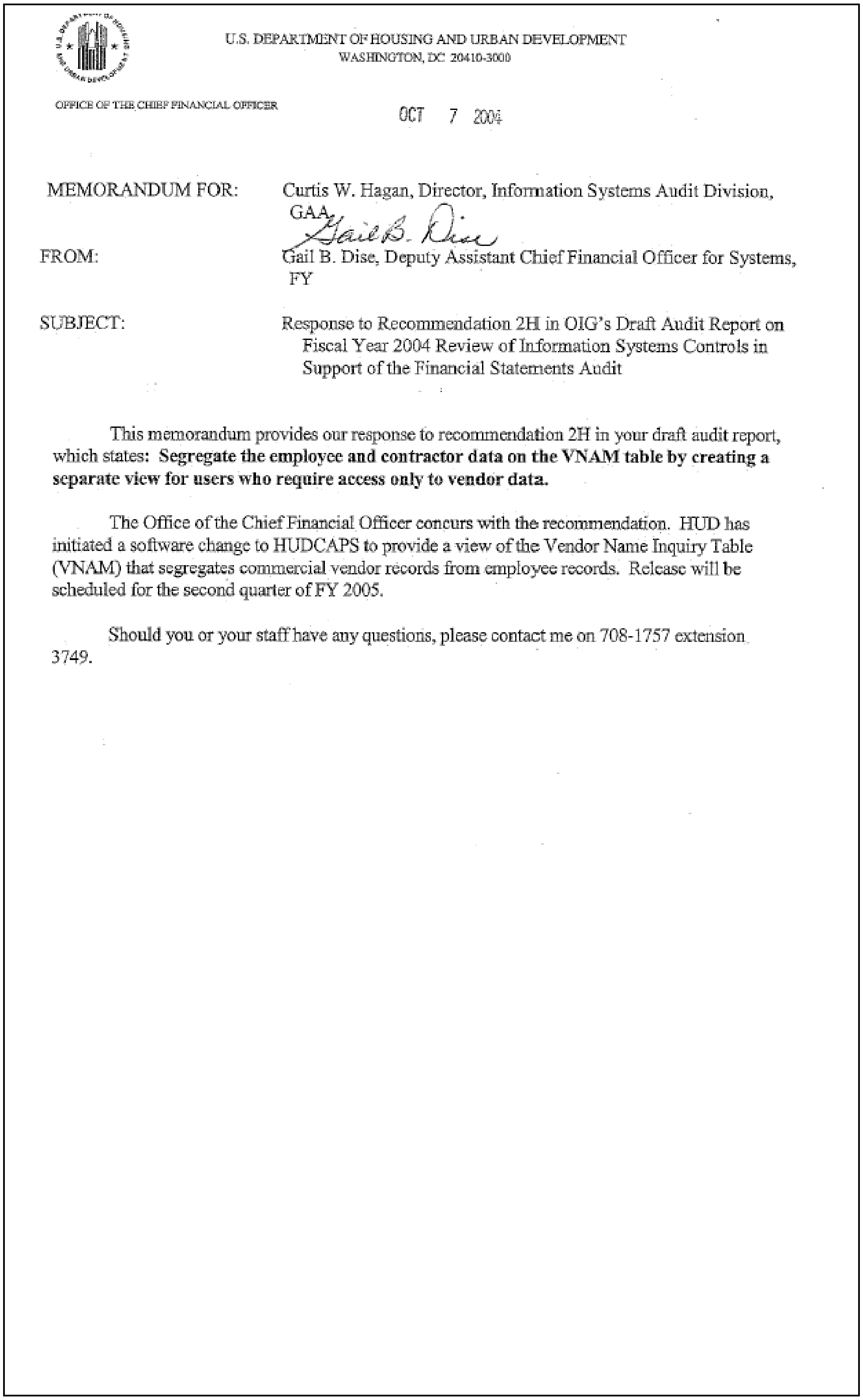
SUBJECT: Response to the Office of Inspector General Draft Audit Report on Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statements Audit

Comment 1

This memorandum responds to your draft audit report, "Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statements Audit," dated September 20, 2004. We have reviewed and concur with all recommendations addressed to our office, except for recommendation 5E, *HUD store backup production data at the EDS Disaster Recovery Facility.* Although we accept recommendation 5E in "principle only", we cannot take the recommended corrective action at this time because it would be cost prohibitive. Due to the protest of the HUD Information Technology Services award, HUD cannot invest in the transfer of production tapes to Electronic Data Systems until after the Government Accountability Office decision is rendered (approximately November 30, 2004).

Thank you for the opportunity to comment on your draft report. If you have any questions concerning this response, please feel free to contact Mary P. Barry, Director, Office of Management and Planning, at (202) 708-1027, extension 123.

Ref to OIG Evaluation **Auditee Comments**



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

OFFICE OF THE CHIEF FINANCIAL OFFICER

OCT 7 2004

MEMORANDUM FOR: Curtis W. Hagan, Director, Information Systems Audit Division, GAA

Gail B. Dise

FROM: Gail B. Dise, Deputy Assistant Chief Financial Officer for Systems, FY

SUBJECT: Response to Recommendation 2H in OIG's Draft Audit Report on Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statements Audit

This memorandum provides our response to recommendation 2H in your draft audit report, which states: **Segregate the employee and contractor data on the VNAM table by creating a separate view for users who require access only to vendor data.**

Comment 2

The Office of the Chief Financial Officer concurs with the recommendation. HUD has initiated a software change to HUDCAPS to provide a view of the Vendor Name Inquiry Table (VNAM) that segregates commercial vendor records from employee records. Release will be scheduled for the second quarter of FY 2005.

Should you or your staff have any questions, please contact me on 708-1757 extension 3749.

OIG Evaluation of Auditee Comments

Comment 1 Comments from the Assistant Secretary for Administration/Chief Information Officer were responsive to our findings and recommendations.

Regarding the response to recommendation 5E, we agree that it be prudent to wait for the GAO decision on the Lockeed Martin bid protest before taking action. A decision from GAO is expected before the end of November 2004. If the bid protest is not upheld and EDS assumes all information technology operations for HUD, our recommendation would become moot since what is now the backup facility (an EDS facility where data is not currently stored) would become the production facility, where all data would be available. EDS would then establish another backup facility where we would expect backup data to be stored.

Comment 2 Comments from the Deputy Assistant Chief Financial Officer for Systems were responsive to our finding and recommendation.

Appendix B

CRITERIA

The Government Accountability Office's "Federal Information System Controls Audit Manual," section 3.1, provides five critical elements for an auditor's use in evaluating an entitywide security program:

(1) Periodic assessment of risks.
(2) Keeping a current, written plan that clearly describes the entity's security program and policies and procedures that support it.
(3) Establishment of a security management structure with adequate independence, authority, and expertise.
(4) Effective, security-related personnel policies.
(5) Monitoring of the security program's effectiveness and making changes as needed.

Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources," provides

> Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Each agency's program shall implement policies, standards, and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration, and the Office of Personnel Management. Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

(1) Assign Responsibility for Security. Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.

(2) System Security Plan. Plan for adequate security of each general support system as part of the organization's information resources management planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology. Security plans shall include:

CONTROLS TO INCLUDE IN SECURITY PLANS FOR	
GENERAL SUPPORT SYSTEMS	MAJOR APPLICATION SYSEMS
Rules of the system	Application rules
Training	Specialized training
Personnel controls	Personnel security
Incident response capability	--
Continuity of support	Contingency planning

Technical security	Technical controls
System interconnection authorization	Protection of shared
--	Public access controls

(3) Review of Security Controls. Review the security controls in each system when significant modifications are made to the system but at least every 3 years.

(4) Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every 3 years.

As explained in NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004:

> **The Federal Information Security Management Act** requires each Federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include
>
> - Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
>
> - Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;
>
> - Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
>
> - Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;
>
> - Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk but no less than annually;

- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;

- Procedures for detecting, reporting, and responding to security incidents; and

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.