Issue Date
December 1, 2003
Audit Case Number
2004-DP-0001

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

Curtis Hagan

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

SUBJECT: Final Audit Report on Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit

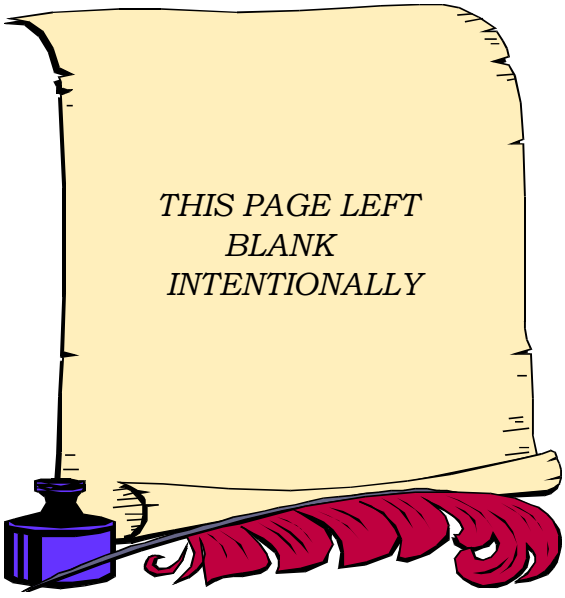
We have completed our review of selected information systems general and application controls in support of the fiscal year 2003 financial statements audit. Our review was based on the General Accounting Office "*Federal Information Systems Controls Audit Manual*," and information technology guidelines established by the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST).

Our review found information systems controls weaknesses that could negatively affect the integrity, confidentiality, and availability of computerized data. This is due to HUD's noncompliance with Federal requirements and standards, as well as HUD's own internal policies and procedures. We recommend that HUD take steps to ensure that OMB requirements, NIST guidelines, HUD's own internal policies and procedures are implemented.

Within 60 days please provide us, for each recommendation without management decisions, a status report on: (1) the corrective action taken; (2) the proposed corrective action and the date to be completed; or (3) why action is considered unnecessary. Additional status reports are required at 90 days and 120 days after report issuance for any recommendation without a management decision. Also, please furnish us copies of any correspondence or directives issued because of the audit.

We appreciate the courtesies extended to the audit staff. Should you or your staff have any questions, please contact me at (202) 708-0614 extension 8149 or Hanh Do at extension 8147.

Attachment


THIS PAGE LEFT
BLANK
INTENTIONALLY

Executive Summary

We have completed our review of selected information systems general and application controls in support of the fiscal year 2003 financial statements audit. Our review was based on the General Accounting Office "*Federal Information Systems Controls Audit Manual*," and information technology guidelines established by the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST).

Our review found information systems controls weaknesses that could negatively affect the integrity, confidentiality, and availability of computerized data. This is due to HUD's noncompliance with Appendix III of OMB Circular A-130, NIST requirements and standards, as well as HUD's own internal policies and procedures as follows:

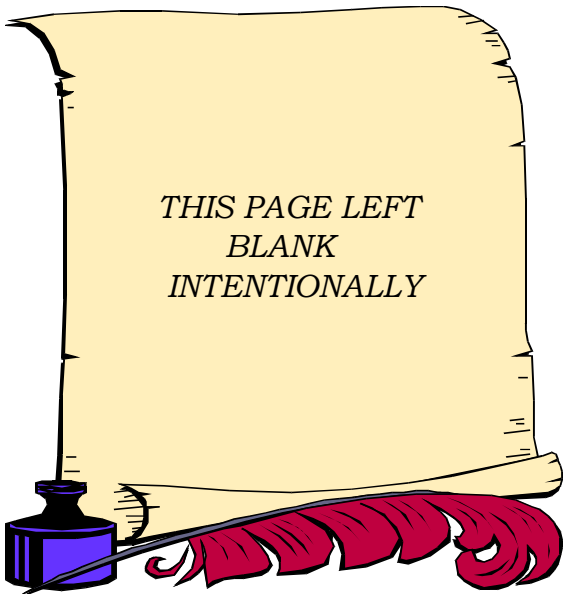
- HUD's entity wide information security planning and management program does not meet the minimum set of controls for automated information resources established by Appendix III to OMB Circular A-130.
- Controls on the IBM compatible Hitachi mainframes and network do not adequately protect data and application programs from potential unauthorized modification, loss, and disclosure.
- Software change management procedures are not being followed, making HUD vulnerable to the introduction of unauthorized programs or changes to application and system software.
- Inadequate segregation of duties exists in system security administration exposing HUD to increased risk of improper activities.
- HUD has not followed NIST guidelines for the development and testing of contingency related plans, resulting in inadequate assurance that HUD can recover computer processing operations in the event of a disaster or other unexpected interruptions.

Recommendations

We recommend that the Assistant Secretary for Administration/Chief Information Officer ensure that OMB requirements and NIST guidelines as well as HUD's own internal policies and procedures are implemented.


THIS PAGE LEFT
BLANK
INTENTIONALLY

Table of Contents


THIS PAGE LEFT
BLANK
INTENTIONALLY

Introduction

The Department of Housing and Urban Development was created in 1965 to increase homeownership, support community development, and increase access to affordable housing free from discrimination. HUD annually subsidizes housing costs for approximately 4.5 million low-income households through rental assistance, grants and loans. It helps revitalize over 4,000 localities through community development programs. HUD encourages homeownership by providing mortgage insurance for more than six million homeowners with low and moderate incomes, many of whom would not otherwise qualify for loans.

Audit Objectives

The overall audit objective was to evaluate the effectiveness of general controls over HUD information systems, on which the financial systems reside, maintained and operated by the Department during fiscal year 2003. These information system controls can affect the security and reliability of financial and other sensitive data including employee personnel data, public housing inventory, and housing tenant family data maintained on the same computer systems as the Department's financial information.

Audit Scope and Methodology

Our review was based on the General Accounting 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 entity wide 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 discussion 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 2002 audit.

We performed audit work at the HUD Headquarters in Washington, D.C.; Data Center in Lanham, MD; and Disaster Recovery Facility in Reston, VA. The audit covered the period October 2002 through September 2003.

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.

Controls Over HUD's Computing Environment Can be Further Strengthened

Our review found noncompliance with the requirements of OMB Circular A-130, Appendix III, guidelines issued by the National Institute of Standards and Technology and HUD's own internal policies and procedures for automated information resources controls. Specifically, (1) the Department needs to improve its entity wide security; (2) access controls need to be improved on the IBM compatible Hitachi and network environments; and (3) Quality Assurance needs to be implemented to improve software change controls.

Background

On March 1, 2002, the Department issued a Request for Proposal to replace the existing HUD Integrated Information Processing Service (HIIPS) contract that expired in May 2003. HIIPS supports all aspects of the acquisition, configuration, installation and implementation of computer hardware, software and telecommunications. Vendor proposals were received during May 2002 and the contract was awarded to a new contractor on August 14, 2003. The new infrastructure contract is named HUD Information Technology Service (HITS). It is a performance-based, outcome-oriented infrastructure contract through a single vendor. There will be a transition period between the current and new contractor during which equipment and workload from the current Disaster Recovery Facility in Virginia and the Data Center in Maryland will be installed and migrated to the new Data Center in West Virginia. A subcontractor will provide disaster recovery services.

Entity Wide Security

The Department has not met the minimum set of automated information resource controls relating to Security Plans, Independent Review of Security Plans, and the Accreditation and Certification of major applications and general support systems. We noted significant noncompliance with OMB A-130 Appendix III requirements as well as requirements and standards issued by the National Institute of Standards and Technology (NIST) and HUD's own internal policies and procedures.

HUD's major applications do not have an initial Authorization to Process or documentation supporting that applications were reauthorized within the last three years.

Contrary to OMB and NIST requirements, HUD's major applications do not have an initial Authorization to Process (referred to as Accreditation and Certification by NIST) or documentation supporting that applications were reauthorized within the last three years. Also, project sponsors are not fully aware of their responsibilities relating to Authorization to Begin Processing or Reauthorizing requirements, and security plans. OMB A-130 Appendix III "*Security of Federal Automated Information Resources,"* and NIST Special Publication (SP) 800-37 "*Guide for the Security Certification and Accreditation of Federal Information Systems,*" requires that a management official must authorize in writing the use of the application or system by confirming that its security plan as implemented adequately secures the application prior to authorizing a major application or general support to begin processing. Also, there must be a re-authorization at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application. OMB and NIST requirements are incorporated into HUD's "*System Development Methodology"* and the HUD Handbook 2400.24 "*ADP Security Program.*"

No evidence that HUD's major application security plans were updated within the last three years.

OIG has not received evidence that HUD's major application security plans were updated within the last three years. We evaluated a sample of HUD's application security plans during FY 2002[1] and recommended that HUD prepare and update security plans to meet Federal requirements. The Department has performed 17 out of 258 security plan reviews but would not make them available to OIG because they are in draft status. However, HUD has indicated that no independent testing was performed and therefore is still not in compliance with NIST. Appendix III of OMB A-130 requires an independent review or audit on the security controls in each major application and general support system be performed when significant modifications are made, but at least every three years.

HUD incorrectly defined its general support system boundaries by classifying all support related information resources as one general support system. These support systems do not share direct management control and/or

[1] Audit Report Memorandum #2002-DP-0002 titled "Review of Department IT Security Plans"

The General Support System security plan is not compliant with OMB A-130 and NIST.

common functionality. In addition, NIST SP 800-18, "*Guide for Developing Security Plans for Information Technology System,*" indicates that general support systems under separate direct management control or with separate functions and missions should have separate security plans. In determining the boundaries of the general support systems, management should consider that each element of the system must have essentially the same operating characteristics and security needs; and reside in the same general operating environment. Finally, depending on the potential risk and magnitude of harm that could occur, Departmental management should consider identifying general support systems security plan deficiencies in its OMB A-123, "*Management Accountability and Control"* and the Federal Managers' Financial Integrity Act (FMFIA) reporting, if there is no assignment of security responsibilities, no security plans, or no Authorization to Process for systems.

HUD does not have system interconnecting agreements between:

- HUD's Central Accounting and Program System (HUDCAPS) and National Finance Center (NFC);
- Tenant Rental Assistance Certification System (TRACS) and Social Security Administration (SSA);
- Single Family Insurance Claims System – Claims Subsystem (SFICS-Claims) and Department of the Treasury.

System interconnection is the direct connection between two or more Information Technology systems for the purpose of sharing data and other information resources.HUD has numerous OS/390 computer mainframe-based financial applications that require interconnecting with the Treasury, NFC, SSA, other financial institutions, and external partners over a wide area network. We requested system interconnecting agreements for HUDCAPS, TRACS and SFIC-Claims and the Department was unable to produce them. The system owners directed us to the Office of the Chief Information Officer (OCIO) for the agreements. We made the request to several offices within the OCIO and were directed back to the system owners.

OMB A-130 Appendix III requires that government organizations obtain written management authorizations for system interconnection and that controls consistent with NIST shall be established. NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*," provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology systems that are owned and operated by different organizations. A weakness at HUD or other government and extranet interconnected partners may open additional network vulnerabilities. If one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other systems.

Hitachi Environment

Administration of user access to system resources needs to be improved.

User access administration needs to be improved. As a result of our audit during fiscal year 2002, HUD agreed to establish a CA-EARL[2] job to assist in security administration by identifying those User-IDs that have not been accessed within six months. We have not seen evidence that the job was created. For example, during May 2003, we reviewed user-Ids for TRACS and found 5 contactors and 40 HUD employee user-Ids that were inactive for more than 180 days. We visited this again during July 2003 and found 2 contractors and 17 HUD employees' user-Ids that were identified during May still on the system. Finally, our review found user-Ids belonging to terminated contractors still on the system. Even though the application program office had submitted requests to remove the user-Ids, there were two contractor user-Ids that have been inactive since September 2002 and one since April 2003. They were deleted when OIG brought it to the Department's attention.

NIST SP 800-14, "*Generally Accepted Principles and Practices for Securing Information Technology Systems,*" indicates that organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. Terminated employees who continue to have access to

[2] CA-Earl is an automated reporting utility that efficiently identifies inactive user IDs on the mainframe.

critical or sensitive resources pose a major threat, especially those individuals who may have left under acrimonious circumstances.

Administration of computer resources needs to be improved.

Administration of computer resources needs to be improved. We found 1,275 datasets belonging to 12 deleted user-Ids still residing on the system. The GAO *Federal Information System Controls Audit Manual* (FISCAM) and the HUD Handbook 2400.24, "*ADP Security Program,*" indicates that the entity should have procedures in place to clear sensitive information and software from computers, disks, and other equipment or media at the end of the contract and when they are disposed of or transferred to another use. HUD's computer operating procedures "*HMIS006 - Deletion of Obsolete Alias's and Associated Resources*," indicates that the ADP Security Office has the responsibility to initiate requests to delete obsolete Alias's and their associated resources from the Hitachi mainframes. Requests should be sent to Data Management who will delete resources (datasets) associated with the ACID(s) as well as their Catalog Alias from the mainframe. If sensitive information is not fully cleared, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media. Also, deletion of the datasets would free up the storage space on the computer and potentially reduce storage cost to the Department.

A system programmer also serves as backup for the security administrator.

A system programmer also serves as backup for the Top Secret[3] administrator. These two job functions should be performed by different individuals. The system programmer should not be allowed to have all the access authorities of a Top Secret administrator. In addition, there is a problem if the individual is not available to perform backup duties because he has other system related priorities. GAO FISCAM indicates that different individuals should perform system programming and data security duties. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

[3] HUD uses Top Secret as the standard security software package to secure the Department's operating system environment under the Hitachi platform.

Not all 15 individuals who have "superuser" authority need the access.

Fifteen system programmers have "SUPERUSER" authority. This authority permits the user to bypass all security checks and access certain Unix System Services resources on the IBM compatible mainframes. Not all 15 individuals require this authority to perform their job functions. The GAO FISCAM indicates that access to system software should be restricted to a very limited number of personnel whose job responsibilities require they have such access. FISCAM also states that entities may have a tendency to authorize access to many individuals so that emergency operating problems can be handled promptly. However, management must balance the need for efficiency with the need for security.

The DB2 system audit trail reports are not reviewed.

Although the DB2 system audit trail is turned on, the reports are not being reviewed because Offices within the OCIO assumed the other parties should be responsible for their review. DB2 is IBM's database software used by HUD to manage data for at least 17 HUD applications to include HUDCAPS and TRACS. In response to a 1997 OIG audit, the Department turned on the DB2 audit trace accounting classes 1 and 2 to track access to DB2 resources. GAO FISCAM and NIST SP 800-14, indicates that audit trails should be reviewed periodically; suspicious activities be investigated; and appropriate action taken. By not reviewing the audit trail, unauthorized, unusual, or sensitive access activities will not be identified and appropriate action will not be taken to identify and remedy the control weaknesses that allowed the violation to occur. Violations could continue to occur and cause damage to HUD'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. HUD has indicated that while the Department currently does not have the staff or expertise to review the audit trail reports, the DB2 system audit trail reports will be reviewed under the HITS contract.

Network Environment

Weaknesses in HUD network security were found during a vulnerability assessment.

A number of weaknesses in HUD network security were found during a vulnerability assessment performed during July by a HUD subcontractor.[4] Some of the weaknesses had been previously reported to HUD following a vulnerability assessment performed from October 29, 2001 through November 5, 2001 by an OIG contractor. OMB A-130 indicates that Agencies shall protect information commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. Also, HUD's Handbook 2400.24 indicates that information processed by HUD networks and associated equipment must be properly safeguarded against unauthorized access, modification, disclosure, destruction, or denial of use.

The SSO InSync software does not use triple DES to encrypt passwords

The HUD implemented Single Sign-on (SSO) InSync software product does not use triple Data Encryption Standard (DES) to encrypt passwords. The Department is in the process of implementing SSO by password synchronization. The password is captured and then sent to the different applications so the user can access many applications without having to sign on more than once. The SSO server software uses Session DES encryption so that a new key is used with each transmission. Encrypted data is sent from the server to the SSO agents. Federal Information Processing Standards Publication (FIPS PUB) 46-3, "*Data Encryption Standard*," indicates that triple DES is the approved symmetric encryption algorithm of choice. The Advanced Encryption Standard (AES) is also a FIPS-approved[5] encryption algorithm that was developed subsequent to DES and could be used in place of triple DES. The SSO vendor intends to upgrade the InSync software to utilize AES in the next product release.

Federally recommended password rules not implemented.

The Department has not implemented certain password rules for the Windows 2000 Operating System as recommended by the NIST, National Security Agency (NSA), and Microsoft as follows:

[4] Due to the sensitive nature of the findings, details of the vulnerabilities identified are not discussed in this report. Requests for the information can be made to the Office of the Chief Information Officer

[5] FIPS PUB 197, "*Advanced Encryption Standard (AES)*"

Rules Description	Implemented HUD Rules	Rules Recommended by NIST, NSA, Microsoft
Min Password Length Non-Sys Admin	6 characters	8 characters
Min Password Length Sys Admin	6 characters	>12 characters, if possible
Password Construction	No special characters	Mix of reg. and special char.
Account Lockout	6 invalid logon attempts	3 invalid login attempts
Enforce Password History	6 passwords	24 passwords

The Department indicated that any additional security technology settings that have an impact on the entire HUD community (approximately 13000 desktops) should be assessed by the new HITS vendor. In addition, HUD choose to implement the current password rules for the following reasons:

- Union agreed to these rules.
- Easy transition from Novell Netware to Server 2000.
- Unisys machine cannot handle an 8-character password.
- Password settings for Server 2000 are compliant with FIPS PUB 118.
- Numeric and upper case characters in the password string addressed a prior OIG audit recommendation to improve password rules.

HUD management is ultimately responsible for the security of the Department's information systems. OMB policy, most recently stated in memorandum number M-03-19 dated August 6, 2003, requires Federal agency procedures to be consistent with guidance issued by NIST when such is available. The NIST guidance for configuring Windows 2000 is given as an example in the OMB memorandum. Failure to strengthen the Windows 2000 server password construction and login policies and implementation practices could allow hackers to compromise the confidentiality, integrity, and availability of information. FIPS PUB 118 referenced by HUD was issued by NIST in 1985 and withdrawn by NIST in March 1992.

Configuration Management

Configuration Management (CM) 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. HUD uses the automated CM management tool called PVCS to control software changes and releases for applications on the client-

server and web applications, and Endevor on the IBM compatible Hitachi mainframe computers. All software changes, including emergency fixes, must go through the CM tools such as PVCS and ENDEVOR.

The Department does not have adequate CM Quality Assurance (QA) and monitoring procedures to review activities to ensure they adhere to established CM plans, standards, and procedures. Below are examples of deficiencies that could have been detected had QA procedures been implemented. Some were corrected after we brought them to the Department's attention:

- HUD has not maintained the integrity and accuracy of Development versus Production software inventories on the Hitachi mainframe. Software discrepancies exist for applications including SAMS and TRACS. Our review found numerous modules that exist in the production environment but are not in the Endevor environment or vice versa. We also found that many same modules in both Endevor and Production environments are not identical.
- The Hitachi mainframe Endevor parameter "Quorum Size" for TRACS allowed developers to move software into the Endevor PROD environment with no independent review and approval process.
- Some client server development contractors were granted excessive privileges in PVCS. A contractor was granted UNLIMITED privilege for the Integrated Automate Travel System. Two contractors were granted UNLIMITED privilege and one contractor was granted SUPERUSER privilege for TRACS.
- The TRACS development team does not follow proper procedures for conducting CM emergency fixes, including the use of maintenance libraries.
- The CM implementation team did not remove access for eight contractors when TRACS submitted the request during February 2003. Their access was removed only after OIG brought it to the team's attention during August 2003.

NIST SP 800-14 indicates that the effectiveness of security controls also depend on such factors as system management, quality assurance, and internal and

management controls. GAO FISCAM indicates that periodic management reviews are essential to make certain employees are performing their duties in accordance with established policies. Monitoring ongoing activities that assess the internal control performance over time ensures that identified deficiencies are reported to senior management. Finally, the "*HUD Quality Assurance Guidelines*" states that: Technical Services may be responsible for establishing and maintaining QA guidelines; QA may be responsible for monitoring project staff activities and processes for compliance with standards and policies; and Project management may be responsible for identifying and ensuring that the quality factors to be implemented in the system and software are fulfilled.

Auditee Comments

HUD concurs with all findings and recommendations except for recommendation 1G. The Department interprets FIPS PUB 46-3 to require implementation of triple DES for new systems only. The Single Sign-on password synchronization product was fully implemented in May 1, 2002. Therefore, HUD does no believe this standard is applicable.

OIG Evaluation of Auditee Comments

FIPS PUB 46-3 is applicable to the Single Sign-on password synchronization product because the standard was reaffirmed and made available for Federal agencies' usage on October 25, 1999, more than two years prior to the SSO implementation date of May 1, 2002.

Our discussions with the product vendor and personnel within the OICO found that the SSO vendor intends to upgrade the InSync component to utilize AES in the next product release. AES is also a FIPS-approved encryption algorithm that was developed subsequent to DES and could be used in place of triple DES. We have revised recommendation 1G to recommend that HUD upgrade the SSO software when the next release is available.

Recommendations

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

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 and HUD's internal standards.

1B. Follow NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*," by:

- Performing Certification and Accreditation to test and evaluate the technical and non-technical security features of the systems.
- Requiring implementation plans to identify and examine all relevant technical, security, and administrative issues surrounding the interconnection for establishing the interconnection.
- Requiring written system interconnecting agreements, to include an Interconnection Security Agreement and a Memorandum of Understanding (or Agreement).
- Ensuring that written system interconnecting agreements are included in the systems security plans.
- Reviewing security controls for the interconnections at least annually or whenever a significant change occurs to ensure they are operating properly.
- 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:

- Implementing a bi-annual (at a minimum) user-ID deletion schedule to remove those user-IDs inactive for more than 6 months. A CA-EARL job to verify the user-IDs inactive for more than 6 months should be established.

- Ensuring that requests to remove departed users' user-ids are carried out and that the requestors are notified of the removal.
- Carrying out procedures to remove resources (datasets) associated with deleted user-ids as well as their Catalog Alias from the mainframe. This includes ensuring that the IT Operations Security Branch initiates the request to the Departmental Platforms and Processing Division, who would notify the Security Branch when the removal is completed.
- 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.

1D. Control and monitor the "SUPERUSER" authority by:

- Developing policies and procedures for the use of ROOT authority on the production mainframe.
- Restricting assignment of ROOT authority to system programmers by limiting it to only those with the need to perform their job function.
- If necessary, developing emergency procedures for assigning users ROOT when needed on a temporary basis.
- Activating audit logging of activities performed by ROOT. The audit logs should also be reviewed for inappropriate and unauthorized activities.

1E. Ensure that the DB2 system audit trail reports are regularly reviewed.

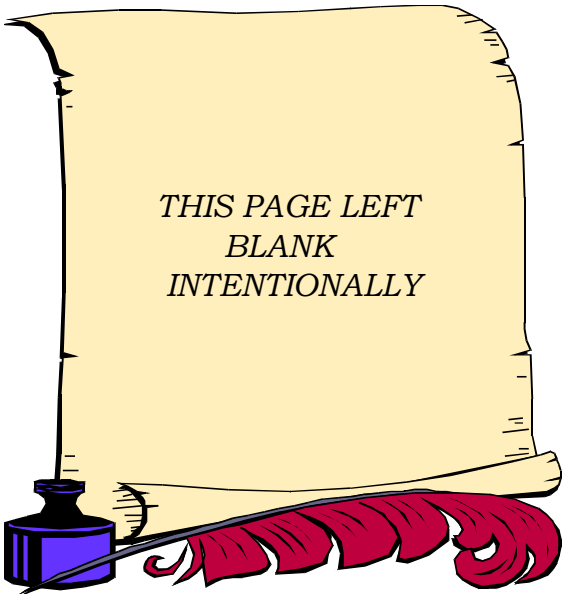
1F. Correct the weaknesses identified by the subcontractor's vulnerability assessment.

1G. Upgrade to the next release of the InSync Single Sign-on software product, that utilizes AES, scheduled for release next year.

1H. Implement the Windows 2000 password rules recommended by NIST, NSA and Microsoft as follows:

- Set the account lockout to 3 invalid logon attempts.
- Set the password history to 24 passwords.
- Set the minimum password length for non-system administrators to 8 characters.
- Set the minimum password length for system administrators to greater than 12 characters, if possible.
- 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 HUD policies and procedures are followed.


THIS PAGE LEFT
BLANK
INTENTIONALLY

Contingency Planning Needs to be Improved

There is inadequate assurance that HUD can recover operational capability in a timely, orderly manner or perform essential departmental functions during an emergency or situation that may disrupt normal operations. HUD needs to revise its current IT contingency planning process to fully utilize the seven steps process as recommended in the NIST SP 800-34, "*Contingency Planning Guide for Information Technology Systems.*" The Department needs to develop or update the following NIST recommended plans: (1) Business Continuity Plan; (2) Business Recovery (or Resumption) Plan; (3) Continuity of Operations Plan; (4) Continuity of Support Plan/IT Contingency Plan; (5) Crisis Communications Plan; (6) Cyber Incident Response Plan; (7) Disaster Recovery Plan; and (8) Occupant Emergency Plan. These plans must take into consideration non-traditional disasters that include massive regional power blackouts like the one that recently occurred on August 14, 2003 and terrorist strikes in the magnitude of the events of September 11, 2001. Finally, HUD needs to test the plans.

Development of Contingency Plans

Current IT contingency planning process does not fully utilize the NIST recommended seven steps process.

The current IT contingency planning process does not fully utilize the seven steps process as recommended in the NIST SP 800-34, "*Contingency Planning Guide for Information Technology Systems.*" For example, The Department could not provide documentation to show that a Business Impact Analysis (BIA) or risk assessments were completed. Therefore, the Department could not support that it incorporates BIAs or identifies preventative controls through risk assessments in the contingency planning process. The Department's IT Contingency Plan (currently called the Business Resumption Plan) includes a list of critical application systems and indicates that the size and hardware requirements of these systems may necessitate a phased operational approach rather than concurrent processing. However, the Plan does not contain guidance on the priority order of restoration on the phased approach. The BIA enables the contingency planning coordinator to fully characterize the system requirements, processes, and interdependencies and uses this information to determine contingency requirements and priorities. HUD will have a BIA completed as part of the newly awarded HITS contract. The results of the BIA should be incorporated into the analysis and strategy development efforts for the Department's Continuity of Operations Plan, Business

Continuity Plan, and Business Resumption Plan. NIST SP 800-34 provides guidance on the seven steps IT contingency planning process to include: (1) Developing the contingency planning policy statement; (2) Conducting a Business Impact Analysis; (3) Identifying preventive controls; (4) Developing recovery strategies; (5) Developing an IT contingency plan; (6) Planning testing, training, and exercises**;** and (7) Planning maintenance.

HUD needs to revise current contingency plans and develop additional contingency related plans.

The Department needs to: (1) adopt NIST SP 800-34 definitions for contingency related plans; (2) revise current plans; and (3) develop additional plans to address areas defined by NIST that are not covered in existing plans. For example, the NIST defined Continuity of Support Plan/IT Contingency Plan is equivalent to HUD's BRP. While the HUD BRP focuses on IT, the NIST defined BRP is not IT focused and addresses recovering business operations immediately following a disaster. The Department does not have a Business Continuity Plan (BCP), as defined by NIST, that focuses on sustaining essential business operations while recovering from a significant disruption. The NIST defined BRP and BCP focuses on business processes and addresses IT based only on its support for business processes. The NIST defined Crisis Communications Plans (CCP) is partially included in the Department's Occupant Emergency plan (OEP). HUD's OEP does not address communications with the public, as recommended by NIST as part of the CCP. The OEP at headquarters is in place along with all satellite offices. HUD is currently reviewing all regional and field offices to determine if all HUD offices have an effective OEP.

NIST SP 800-34 defines the various contingency plans that should be used and developed to include: (1) Business Continuity Plan; (2) Business Recovery (or Resumption) Plan; (3) Continuity of Operations Plan; (4) Continuity of Support Plan/IT Contingency Plan; (5) Crisis Communications Plan; (6) Cyber Incident Response Plan; (7) Disaster Recovery Plan; and (8) Occupant Emergency Plan. NIST indicates that IT contingency planning fits into a broad emergency preparedness environment that includes organizational and business process continuity and recovery planning. The organization would use a suite of plans to properly prepare response, recovery and continuity

activities for disruptions affecting IT systems, business processes and the facility. Because there is an inherent relationship between an IT system and the business it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

The Department has indicated that the new HITS contract is a performance-based contract and that the contractor is charged with providing IT disaster recovery services.However, HUD is not in a position to tell the contractor how to meet these requirements, but only that they must meet the agreed to service levels. Therefore, HUD cannot insist on documents outside of the contract scope. The Department will validate the contractor's solution during the Transition Phase of the HITS contract.

HUD management is ultimately responsible for contingency planning to recover services after an emergency or service interruption. Responsibility includes compliance with Federal contingency planning mandates and statutes such as Appendix III of OMB A-130 and NIST. While the Department has developed certain contingency related plans, not all plans prescribed by NIST have been developed. The HITS contract indicates that the contractor shall comply with all HUD, OMB, and applicable Federal information technology standards and documents including all changes in laws, regulations, policies and procedures as they evolve during the period of contract performance. OMB A-130 Appendix III states that security planning, which includes continuity of support planning, shall be consistent with guidance issued by NIST.

The BRP was not updated to take into consideration non-traditional disasters that include massive regional power blackouts and terrorist strikes in the magnitude of the events of September 11, 2001.

Updates to Contingency Plans

The Department has not updated the BRP to take into consideration non-traditional disasters that include massive regional power blackouts like the one that recently occurred on August 14, 2003 and terrorist strikes in the magnitude of the events of September 11, 2001. The power blackout affected more than 50 million people over a 9,3000-square-mile area in eight states and the Canadian province of Ontario. The current BRP assumes that the HUD Headquarters, HUD Data Center, and Disaster Recovery

Facility will not be impacted at the same time. In addition, significant time delays are not factored into current plan assumptions regarding the availability of highways, airports, trains, buses, police, fire, rescue, and key personnel. The impact of the recent August 14th massive blackout and September 11th attacks suggest that more than one facility can be impacted at the same time and that significant delays may be experienced with respect to the availability of highways, airports, trains, buses, police, fire, rescue, and key personnel.

Previous widely used contingency plan assumptions are no longer reasonable, if they are being used for planned scenarios depicting major disasters. Contingency plans need to consider a wide range of new scenarios that had been seen as remote possibilities but whose probabilities now appear to have increased. Previous planning assumptions on the availability of most key people, regional public transportation systems, primary vendors and the time period to recover critical computer systems are no longer necessarily valid and must be revisited. Willful destruction can occur any place and at any time, on a large or small scale. Implementation of the current BRP may not be affective if the level of actual disruption or disaster, prior to implementation of the HITS contract, is outside of the Department's level of preparedness.

NIST SP 800-30, "*Risk Management Guide for IT Systems,"* provides guidance for risk assessment, risk mitigation, and the continual evaluation process and keys for implementing a successful risk management program. Risk management forms the basis for contingency planning because it is developed in anticipation of a possible event and then executed after that event has occurred. Finally, NIST SP 800-26, "*Security Self-Assessment for Information Technology Systems*," provides a checklist to assist in determining the viability of contingency planning elements. Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission.

Testing of Contingency Plans

Inadequate assurance that HUD can recover from an emergency or situation that may disrupt normal operations.

There is inadequate assurance that HUD can recover operational capability in a timely, orderly manner or perform essential departmental functions during an emergency or situation that may disrupt normal operations. The Department has developed a Continuity of Operations Plan (COOP) for the headquarters and all regional and field offices; selected the alternate site in Richmond, Virginia; and completed a five-year COOP Test, Training, and Exercise (TT&E) plan. HUD has indicated these plans are current and are updated quarterly. However, while the Department has conducted COOP team training and tested the COOP alert notification procedures, the annual test of operations from the alternate site has not been completed due to lack of funds. Federal Preparedness Circular 65 requires internal agency testing and exercising of the COOP plans and procedures to occur at least annually. This ensures agency's ability to perform essential functions and operate from designated alternate facility(ies). In addition, testing of alert notification procedures and systems for any type of emergency should occur at least quarterly.

Annual testing of the BRP was suspended during 2003 due to anticipation of the new HITS contract award.

Annual testing of the Business Resumption Plan (BRP) was suspended during 2003 because the new HITS contract will alter the IT infrastructure. NIST SP 800-34 states that contingency considerations should not be neglected because a computer system is retired or another system replaces it. Until the new system is operational and fully tested (including its contingency capabilities), the original system's contingency plan should be ready for implementation. NIST recommends that existing contingency plans be tested at least annually and when significant changes are made to the IT system, supported business processes, or the IT contingency plan. Each element of the contingency plan should be tested first individually and then as a whole to confirm the accuracy of recovery procedures and the overall effectiveness.

Auditee Comments

HUD concurs with all findings and recommendations.

OIG Evaluation of Auditee Comments

HUD has concurred with all findings and recommendations.

Recommendations

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

2A. Adopt NIST SP 800-34, "*Contingency Planning Guide for Information Technology System,"* for developing contingency related planning as follows:

- Adopt the seven steps.
- Adopt definitions for the various contingency related plans.
- Developing 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/IT Contingency Plan; (5) Crisis Communications Plan; (6) Cyber Incident Response Plan; (7) Disaster Recovery Plan; and (8) Occupant Emergency Plan.

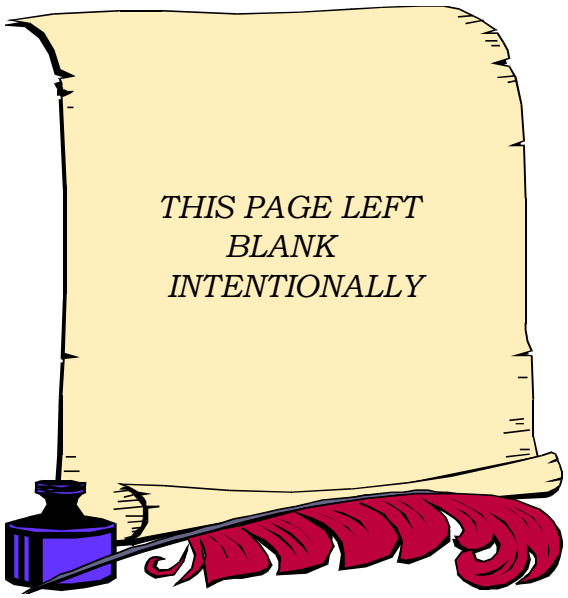
2B. Ensure contingency related plans be updated or developed to take into consideration non-traditional disasters such as massive regional power blackouts like the one that recently occurred on August 14, 2003 and terrorist strikes in the magnitude of the September 11, 2001 attack. For example, plan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

2C. Ensure testing is conducted on contingency related – plans by:

- Testing the COOP at the alternate site as outlined by FPC 66, *Test, Training, and Exercise Program for Continuity of Operations*.
- 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 HITS Data Center in West Virginia.

- 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 the overall effectiveness. Testing should occur at least annually and when significant changes are made to the IT system, supported business processes, or the IT contingency plan.


THIS PAGE LEFT
BLANK
INTENTIONALLY

Weak Personnel Security Practices Continue to Pose 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 FY 2002 and 2001 financial statements, we found that additional weaknesses exist in the Department's management of its personnel security function. Of the 86 users that we identified last year as having greater-than-read access, all except two contractors had been removed from the greater-than-read user access list. Background investigations have been initiated for those individuals. An application controls review of TRACS found that although the IT Operations Security Branch does require users to submit proper user access forms before they are allowed read only access to a system, the application system security administrator can grant greater-than-read access to specific applications without notifying the IT Operations Security Branch or the Office of Emergency and Security Planning.

Personnel Security

For several years we have reported that HUD's personnel security over critical and sensitive systems' access has been inadequate. Although HUD has made some progress to address the reported problems, risks of unauthorized access to the Department's critical financial systems remain a major concern. Without adequate personnel security practices, individuals may be inappropriately granted access to HUD's information and resources that could result in destruction or compromise of critical and sensitive data.

HUD Handbook 2400.24 specifies that the Information Security Staff shall provide oversight on security issues within the Department including system authorization and all other activities and documents required by Federal Laws, regulations, and directives. It also states that the Security Administrators appointed by the System Owners will review quarterly, with assistance from the Information Security Staff, all user-Ids issued to determine if all users still have a valid need to access at current level of privilege.

HUD Handbook 732.3, "*Personnel Security/Suitability*," states that Contracting Officer Technical Representatives and Government Technical Representatives are responsible for: collecting (background investigation) certifications from vendor staff who require mission-critical (sensitive) systems above query access and forwarding them through

Security Administrators to OIT so that access can be granted; notifying Security Administrators when continued access should be denied for vendor staff when they have failed to obtain re-certification for above query access to mission-critical (sensitive) systems; and notifying Security Administrators when a contract terminates or when contractors separate, and there is no longer a need for access to mission-critical (sensitive) systems. The Handbook also states that the Personnel Security Office is responsible for reconciling, as needed, the Security Control and Tracking System (SCATS) database[6] with the IT listing of users who require above query access to mission-critical (sensitive) systems.

Although improvements have been made and corrective actions have been taken to address recommendations as reported in last year's report on the FY 2002 and 2001 financial statements, we found that additional weaknesses exist in the Department's management of its personnel security function. This conclusion is based on a follow-up on the status of the Department's implementation of recommendations made in last year's report and work performed on an audit of application controls of the TRACS. The TRACS is an integrated financial management system developed to address material weaknesses in the financial control of the project-based rental assistance programs administered by the Office of Housing. It is a major application system with a sensitivity rating of S4 (Major Risk) and therefore, considered a sensitive system. Users requesting above-read access to sensitive systems must have a background investigation prior to being granted access privileges.

We conducted follow-up work to determine whether the OCIO has removed greater-than-read access to sensitive systems for the 86 users that we identified last year as having greater than read access. We found that all except two contractors had been removed from the greater-than-read user access list. According to the Office of Security and Emergency Planning (OSEP), background investigations have been initiated for those individuals.

[6] The SCATS database tracks background investigations for all HUD employees and contractors working in sensitive positions or employees who require certification for access to sensitive systems.

We also followed up on the status of the Department's implementation of recommendations made last year. We found that although the IT Operations Security Branch does require users to submit proper user access forms (HUD Form 22017) before they are allowed read only access to a system, the application system security administrator can grant greater-than-read access to specific applications without notifying the IT Operations Security Branch or the OSEP. In essence, although OCIO may be enforcing the policy, the process is not working as it pertains to granting greater-than-read or upgrading access privileges at the application level.

Our review found that OCIO does provide OSEP with a list of users who have access to the Hitachi and Unisys mainframes for reconciliation purposes and that the OSEP does use this list to compare against the data residing in the personnel security's database (SCATS) on a periodic (at least quarterly) basis. However, this reconciliation cannot be accurate if the access security data being provided is not accurate and complete. Specifically, the IT Operations Security Branch does not track users with greater-than-read access at the application level nor is there any mechanism or system in place that would support this effort. As a result, there are instances where users with greater-than-read access at the application level do not have background investigations.

Our audit of application controls of TRACS found 37 out of 870 TRACS users with greater-than-read access privileges who do not have background investigations. The finding indicates that inappropriate access to TRACS was granted because (1) 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 (at the application level) is not being adhered to; (2) there is no automated system or mechanism in place that requires the TRACS Security Administrator to coordinate with the IT Operations Security Branch and OSEP prior to granting a user greater-than read access privileges; and (3) the IT Operations Security Branch does not have a central repository that would serve as a master inventory tracking system to track all users' access levels for HUD's general support and application systems. As a result, unauthorized users have access to

sensitive and critical data and may cause damage, misuse or interact in fraudulent activities and compromise the confidentiality, integrity, and availability of the critical and sensitive data. Details on the finding and recommendations are discussed in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

Auditee Comments

Auditee comments will be provided in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

OIG evaluation of auditee comments will be provided in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

Recommendations

The recommendations for this finding will be made in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

Security Control Weaknesses Were Found in the PIC & TRACS Applications

Our audits of the security controls of HUD's Public and Indian Housing Information Center (PIC) and the Tenant Rental Assistance Certification System found weakness in both applications. The review of PIC found: (1) security planning in the system life cycle for the PIC system was inadequate; (2) comprehensive system sensitivity and risk assessments were not performed in the initiation and development/acquisition phases of the system life cycle; and (3) comprehensive security policy and goals were not prepared in formulating the design of the security aspects of the PIC system. The review of TRACS found weaknesses in the areas of (1) protection of the TRACS database, production data files, and programs; (2) software change controls; and (3) user and system administration access controls.

Our audits of the security controls of PIC and TRACS found weakness in both applications. We have completed the review of PIC, and issued the audit report on September 10, 2003 under the title "*Public and Indian Housing Information Center,"* report #2003-DP-0001. The review of TRACS is currently ongoing and the audit report has not been issued. The recommendations are not incorporated into this report, but will be included in the individual applications' audit report.

Public and Indian Housing Information Center

Public and Indian Housing Information Center

PIC is designed to facilitate a more timely and accurate exchange of data between Public Housing Authorities (PHAs) and local HUD offices by allowing PHAs to electronically submit information to HUD. Since its inception in December 1999, more than 600 transactional web pages have been created; a detailed inventory of 1.3 million public housing units was established; and tenant family data for 3.5 million households was gathered. PIC represents the largest Internet-based system in HUD with over 3.6 million lines of code. There are approximately 4,000 user logins each day made by over 12,000 authorized HA and HUD users. These users upload over 800 files to PIC daily, with the PIC system processing over thirty thousand Family Reports (form HUD-50058s), which equates to over one million transactions per day.

The audit was limited to a review of the PIC Security Maintenance sub-module which controls user access for more than 12,000 users utilizing three separate databases. It allows PIC security administrators to create and maintain users and user roles. PIC security administrators assign roles to users and determine which user roles have access to the different entities and security levels within the respective system modules.

We found that security planning in the system life cycle for the PIC system was inadequate. Comprehensive system sensitivity and risk assessments were not performed in the initiation and development/acquisition phases of the system life cycle. Additionally, we found that a comprehensive security policy and goals were not prepared in formulating the design of the security aspects of the PIC system. As a result, several operational and technical security control weaknesses were found during the audit. Specifically, we found:

1. Inadequate PIC system design structure and documentation has impeded PIH's ability to monitor and control users' computer access;
2. No comprehensive process has been established to monitor and control PIC user access;
3. Access controls over the Security Administration sub-module are not adequate;
4. Separation of duties are needed over the System Administration function;
5. Inadequate controls exist over confidential and sensitive PIC data;
6. Access controls need to be strengthened to identify and authenticate users to the PIC application and database; and
7. System and application audit logs are not being utilized for security and system maintenance purposes.

Without adequate security controls over the PIC system, HUD is at risk that data errors and omissions and system disruptions could occur, and that the system could be exploited by unauthorized individuals for fraud and identity theft as well as the potential for destruction of data by malicious hackers and disgruntled employees.

Tenant Rental Assistance Certification System

Tenant Rental Assistance Certification System

TRACS is an integrated financial system developed to address the material weaknesses in the financial control of the project-based rental assistance programs administered by the Office of Housing. These programs include Section 8, Rental Supplemental, Rental Assistance Program, Section 236, Section 202, and Section 811. The goal of TRACS is to collect tenant data for all programs and automatically provide payment for subsidy programs where HUD is the contract administrator – based upon the contract and tenant data resident in the system. TRACS accomplishes these goals through its subsystems: the Voucher/Payment, Tenant Business, Contract Business, Social Security/ Supplemental Security Income Data Match, and Automated Renewal and Amendment Management Subsystem (ARAMS).

Our audit of TRACS focused on reviewing the effectiveness of the system security access controls to ensure that data is protected against errors, loss, or unauthorized use. We found that:

1. Security controls over the TRACS database, production data files, and programs need improvement
2. Software configuration management needs improvement
3. Contractors were granted excessive access privileges to TRACS
4. Weak personnel security practices pose a risk of unauthorized access to TRACS
5. Adequate system-specific security training has not been provided
6. There is a lack of segregation of duties between key security personnel functions
7. There is a lack of audit trails at the application level to detect security violations, performance problems, or to monitor and log user activities
8. The Test Center's ID and password for the TRACS client server were revealed in the HUD Application Release Tracking System release document.

Well-chosen security rules and procedures protect important assets and support the organizational mission. They can reduce the frequency and severity of computer security-related losses.

Auditee Comments

Auditee comments relating to the PIC system were provided in Audit Report Number 2003-DP-0001, "*Public and Indian Housing Information Center,*" dated September 10, 2003. Auditee comments pertaining to TRACS will be made in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

OIG Evaluation of Auditee Comments

OIG evaluation of auditee comments relating to the PIC system were provided in Audit Report Number 2003-DP-0001, "*Public and Indian Housing Information Center,*" dated September 10, 2003. OIG evaluation to auditee comments pertaining to TRACS will be made in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

Recommendations

Recommendations for the PIC system were made in Audit Report Number 2003-DP-0001, "*Public and Indian Housing Information Center,*" dated September 10, 2003. Recommendation for TRACS will be made in the "Audit of Application Control Review of the Tenant Rental Assistance Certification System" audit report to be issued at a later date.

Auditee Comments

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

ASSISTANT SECRETARY FOR
ADMINISTRATION/CHIEF INFORMATION OFFICER

NOV 25 2003

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

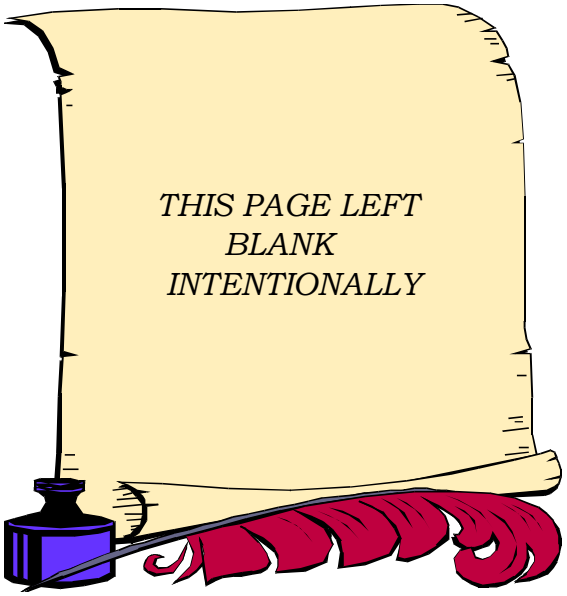
FROM: Vickers B. Meadows, Assistant Secretary for Administration/ Chief Information Officer, A

SUBJECT: Response to Office of Inspector General Draft Audit Report on Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit

This memorandum is in response to the draft audit report, "Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit," dated October 24, 2003. We have reviewed the report and concur with all findings and recommendations except recommendation 1G.

Concerning recommendation 1G, we interpret the Federal Information Publication Standards 46-3 to require implementation of triple Data Encryption Standard (DES) for new systems only. The Single-Sign-on password synchronization product was fully implemented in May 1, 2002; therefore, we do not believe this standard is applicable.

Should you have any questions, please call Mary P. Barry on (202) 708-1027.


THIS PAGE LEFT
BLANK
INTENTIONALLY

Distribution

The Honorable Susan M. Collins, Chairman, Committee on Government Affairs
The Honorable Thomas M. Davis, III, Chairman, Committee on Government Reform
The Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform