
AUDIT REPORT



APPLICATION CONTROL REVIEW OF THE TENANT RENTAL ASSISTANCE CERTIFICATION SYSTEM (TRACS)

2004-DP-0002

February 25, 2004

INFORMATION SYSTEMS AUDIT DIVISION
OFFICE OF AUDIT, WASHINGTON, DC



Issue Date February 25, 2004

Audit Case Number 2004-DP-0002

TO: John C. Weicher, Assistant Secretary for Housing, Federal Housing Commissioner, H
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 Application Control Review of the Tenant Rental Assistance Certification System (TRACS)

We have completed an audit of management, operational, and technical controls over the security of HUD's Tenant Rental Assistance Certification System (TRACS).

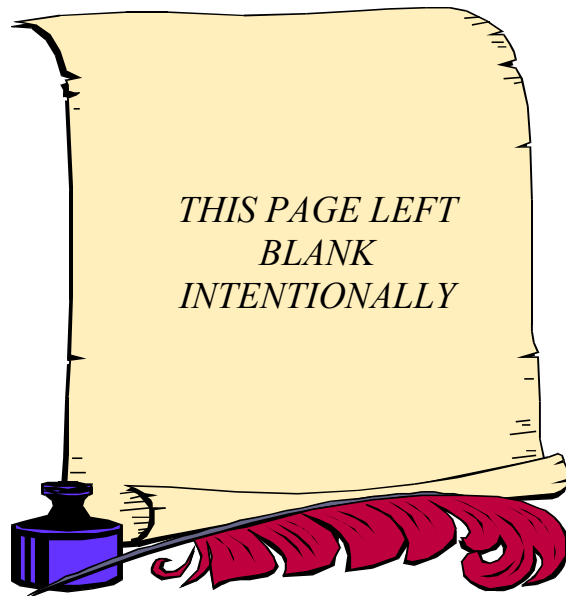
Our report contains six findings with recommendations requiring action by your office. The findings address:

- inadequate access controls over the TRACS data and resources,
- inadequate controls over software configuration management,
- lack of security training,
- inadequate review of audit logs to detect security violations, performance problems, or to monitor and log user activities,
- weak personnel security practices, and
- a lack of segregation of duties.

Within 60 days please provide us, for each recommendation without management decisions, a status report on: (1) the corrective action taken; (2) 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 directive issued because of the audit.

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

Attachment



Executive Summary

We have completed an audit of management, operational, and technical controls over the security of the Tenant Rental Assistance Certification System (TRACS). TRACS is a HUD mission critical financial¹ and program information system that interfaces with other HUD systems. It receives HUD's highest ratings for sensitivity and criticality. Its goal is to collect tenant data for all Housing programs and to automatically provide payment for subsidy programs, where HUD is the contract administrator, based upon the contract and tenant data resident in the system.

We found deficiencies and weaknesses in controls over TRACS security:

- Access controls over the TRACS data and resources are inadequate.
- Controls over software configuration management are inadequate.
- Adequate security training has not been provided.
- Audit logs are not being utilized to detect security violations, performance problems, or to monitor and log user activities.
- Personnel security practices pose a risk of unauthorized access to TRACS.
- There is a lack of segregation of duties performed by key personnel.

The effect of the deficiencies and weaknesses in controls is exposure of TRACS data to unnecessary risk of loss of confidentiality, integrity, and availability.

The Office of Multifamily Housing has taken action to correct some of the weaknesses identified during our review. However, additional corrective action is needed.

Recommendations

Our report contains recommendations for the Assistant Secretary for Housing and the Assistant Secretary for Administration/Chief Information Officer to improve controls over the security of TRACS.

Auditee Comments

The Assistant Secretary for Housing concurred with:

- Finding 1 and Recommendations 1A, 1B, 1C, 1D
- Finding 3 and Recommendations 3A, 3B, Recommendation 4
- Finding 5 and Recommendation 5C.

The Assistant Secretary for Housing partially concurred with:

- Finding 2 and Recommendation 2B and 2C
- Finding 4

¹ HUD has identified TRACS as a “mixed system,” a term defined in OMB Circular A-127 as an information system that supports both financial and nonfinancial functions.

- Finding 6 and Recommendations 6A and 6B.

The Assistant Secretary for Administration/Chief Information Officer concurred with all applicable recommendations. See Appendix A for auditee comments.

Table of Contents

Management Memorandum	i
-----------------------	---

Executive Summary	iii
-------------------	-----

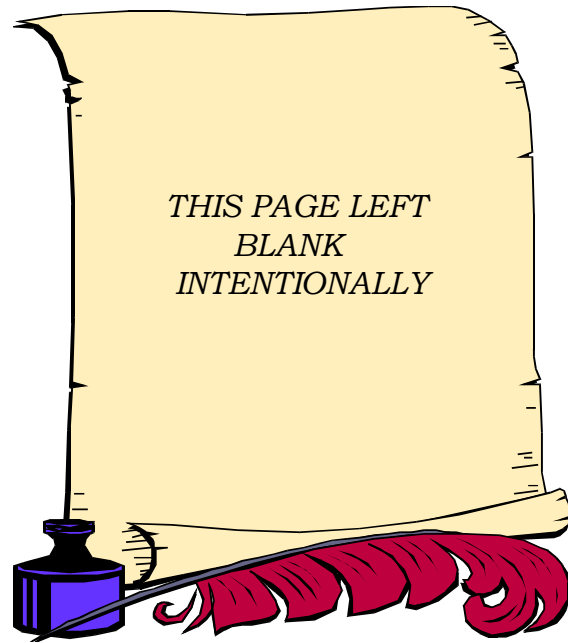
Introduction	1
--------------	---

Findings

1. Access Controls Over TRACS Data and Resources Are Inadequate	3
2. Controls Over Configuration Management are Inadequate	9
3. Security Training Has Not Been Adequate	15
4. Audit Logs Are Not Properly Used	21
5. Weak Personnel Security Practices Risk Unauthorized Access to TRACS	25
6. Duties of Key Personnel Should be Segregated	29

Appendix

A. Auditee Comments	35
B. Distribution	48



Introduction

In 1992 the Department of Housing and Urban Development (HUD) implemented the Tenant Rental Assistance Certification System (TRACS). The purpose of TRACS was to improve fiscal control over Section 8 and other assisted Housing programs. It was designed to process subsidy contracts, tenant rental assistance information, and owner requests for payment (vouchers). TRACS is used to collect tenant data and voucher data for project-based programs and to authorize payment for these programs. The Office of Housing, Assistance Contract Administration Oversight, is the owner of TRACS.

TRACS has approximately 20,000 users. This includes HUD employees, contractors, owners, management agents, state agencies, and contract administrators of subsidized multifamily projects. TRACS processes data for approximately 250,000 payments made annually to contract administrators and project owners of multi-family and project-based rental assistance programs that are administered by the Office of Housing. Total annual payments are approximately \$6 billion. Programs administered by the Office of Housing include Section 8, Rent Supplemental, Rental Assistance, and Section 202 Elderly and Disabled subsidy payments. TRACS serves as the sole repository of tenant certifications, vouchers, and contract data for HUD's Multifamily Housing.

TRACS is a HUD mission critical financial system, which interfaces with other HUD systems. It received HUD's highest ratings for Sensitivity (S4) and Criticality (C4). TRACS processes information whose loss, misuse, improper disclosure, or modification would have a debilitating impact on the mission of the agency. Data collected and processed through TRACS must be available on a timely basis to meet mission-reporting requirements and provide timely payment requests to another HUD financial system, the Line of Credit Control System (LOCCS).

Audit Objectives

The objective of our audit was to assess the adequacy of management, operational, and technical controls over the security of HUD's Tenant Rental Assistance Certification System (TRACS).

Audit Scope and Methodology

The scope of our audit included controls over access to TRACS and controls over changes to system software. We selected 2 production libraries and reviewed 16 module changes associated with these libraries. We also reviewed the personnel security practices as it relates to access controls for 870 TRACS users to determine whether these users had background investigations prior to being granted greater-than-read access to TRACS data and resources. We found 37 exemptions. We conducted interviews with various Housing program personnel. We reviewed documents on TRACS design and database specifications, configuration management, production access, and security.

We reviewed user guides for the TRACS Internet application and Monthly Activity Transmissions. We also reviewed HUD's data quality assessment of TRACS.

We received a demonstration of the system to obtain an overall understanding of its business functions.

We used the following publications as criteria for our assessment of controls:

- Office of Management and Budget (OMB) Circulars A-123 and A-130,
- HUD Handbook 2400.24 REV-2, "Information Security Program."
- Federal Information System Controls Audit Manual (FISCAM),
- Federal Information Processing Standards (FIPS) Publication 73, and
- National Institute of Standards and Technology (NIST) guidance.

We obtained additional documentation, conducted testing, and performed analyses as necessary to accomplish our audit objectives.

Our conclusions are based on our analysis of the documentation obtained, results of the tests we performed, and interviews we conducted.

We performed audit work at HUD Headquarters and selected user sites. The audit covered the period from March 2003 through September 2003.

The audit was conducted in accordance with generally accepted government auditing standards.

Access Controls Over TRACS Data and Resources are Inadequate

We found that access controls over the TRACS data and resources are inadequate. Planned or written security controls over the TRACS database, production data files, and programs have not been properly implemented. As a result, several individuals received a level of access to TRACS that exceeded what was needed to perform their functions.

We also found that key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions were not adequately separated among TRACS security personnel.

Criteria

National Institute of Standards and Technology (NIST) Special Publication (SP) Number 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states that organizations should ensure effective administration of user's computer access to maintain system security. Organizations should implement access controls using the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions. Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts, (2) tracking users and their respective access authorizations, and (3) managing these functions. In addition, the NIST publication states that it is necessary to periodically review the levels of access each individual has, conformity with the principle of least privilege, whether all accounts are still active, and whether management authorizations are up to date. Additionally, an organization should consider both internal and external access control mechanisms. Internal access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. External access controls are a means of controlling interactions between the system and outside people, systems, and services. One of the access control mechanisms that can be used is the access control lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted.

HUD Handbook 2400.24 REV-2, "Information Security Program," dated November 10, 1999, established the following security policies:

- System owners are responsible for decisions regarding the security of application systems and will have the lead role in ensuring that the Security Administrator reviews quarterly, with assistance from the information security staff (IT Operations Security Branch), all user accounts (user IDs) issued to determine if all users still have a valid need to access at current level of privilege.
- The Security Administrator will identify individuals having access to application systems with assistance from the Office of Information Technology.
- The Office of Information Technology shall be responsible for providing access to database resources while preserving access control.
- Upon relinquishing contractor personnel who have access to sensitive information, the Government Technical Representative will inform all staff members who need to know that the individual has been officially removed from information system access.
- The Information Security Staff (IT Operations Security Branch) will perform central administration duties for the access control systems in place.
- System owners, in coordination with program supervisors and Security Administrators, will ensure that system access is based on the need to perform specific job functions.

Written policies and procedures for access controls have not been implemented

Security controls over the TRACS database, production data files, and programs have not been properly implemented. For example, HUD uses contractors to maintain and operate the system software and databases. However, we found that 14 out of 21 contractor support personnel had access privileges that were not necessary to perform their specific job functions. For example, some contractors had unnecessary access privileges to TRACS data files within the production environment. This condition occurred because the IT Operations Security Branch granted greater-than-read access² to contract support personnel upon the request of the Government

² Greater-than-read access privileges may allow an individual the ability to delete, insert, and/or modify data.

Technical Monitor rather than upon approval of the system owner or security administrator.

In other instances, contractor support personnel were inadvertently granted excessive access through the assignment of a user ID that was defined within a Profile³ ID that concurrently allowed unnecessary access to data sets and production libraries.

We found that one user was inadvertently granted excessive privileges that would allow him to delete, insert, and update TRACS data as well as allow him to grant access privileges to other unauthorized personnel. According to TRACS security personnel and management, they were unaware of this user's unauthorized excessive access privileges. They expressed their concern about this situation and considered this issue a high risk to the TRACS. Corrective action by the auditee was taken to remove the user's excessive privileges during the audit.

Departed contractor personnel still had access to TRACS

We found seven contractor support personnel who were no longer working on the TRACS project and no longer had a need for access to TRACS yet still had access. We found that three departed contractors still had access to TRACS data and resources because the IT Operations Security Branch was neither consistent nor prompt in responding to notifications to remove departing contractors. In other instances, the TRACS Hotline Manager was neglectful in immediately sending requests to the IT Operations Security Branch to remove access for four departed or terminated contractors. Also, the IT Operations Security Branch:

- did not always send deletion requests to the appropriate offices, informing them that they can proceed with the removal of specific User IDs and resources (datasets) associated with the deleted User IDs from the mainframe,
- did not use the automated reporting facility called CA-EARL to identify inactive User IDs for removal, and
- did not adhere to their in-house developed User ID deletion schedule.

³ In CA-Top Secret, profiles are established as a set of common resource access characteristics. They are used when a group of users need to use a set of identical resources in the same way and/or the users perform similar or related job functions. It is convenient to define this set of access authorizations once and then associate the entire set with each of the users in the group

Corrective action to remove users' access privileges was taken during the audit upon our notification to the auditee of these findings.

Data sets are not accurate and current

We found that the datasets⁴ listed in the TRACS Profile ID "F87PSELC" do not represent the most currently existing data sets. Specifically, our review showed that some data sets were obsolete.⁵ This condition occurred because upon deleting data file sets listed under the TRACS Profile ID "F87PSELC," the contractor's System Management Group did not notify the IT Operations Security Branch once the deletions were completed.

Accurate user access control lists are not maintained

We found that access control lists (ACLs) that identified all TRACS users and the type of access they were given were not being maintained. HUD uses ACLs as an access control mechanism that registers users who have been given permission to use a particular system resource and the types of access they have been permitted. However, HUD has not maintained ACLs. For example, we found a total of 107 users who were identified on the ACL as having greater-than-read access to the mainframe who no longer had access. This adversely impacts the accuracy of the mainframe user ACLs. According to the TRACS Security Administrator, maintaining an accurate ACL has been a challenge because the IT Operations Security Branch does not consistently provide him with sufficient reports showing the status of a user's access privileges. Nor is there an automated mechanism or process in place that would allow him to verify the accuracy of the ACLs. Rather, he manually maintains his user access lists by consolidating different reports provided by different offices. Without accurate ACLs, the TRACS Security Administrator is unable to conduct accurate quarterly reviews of all User IDs that have been issued to determine if all users still have a valid need to access at their current level of privilege.

We found other instances in which users were allowed access to data and privileges in excess of what was needed to accomplish their job functions. Specifically, we found that there are eight HUD contractors who have unnecessary

⁴ A dataset is a data file or collection of interrelated data. The term is used in the mainframe community, whereas file is used almost everywhere else. A data set in an IBM mainframe is the equivalent of a file in other operating systems.

⁵ The obsolete data sets found were "F87.DSNBUILD., F87.GRAY, F87.OUT., and F87.SUM."

Users had access privileges in excess of what was needed for their jobs

access privileges to functions that allow them to update the Automated Renewal and Amendment Subsystem ((ARAMS)—a subsystem of TRACS) data and perform financial processes including processing funding and obligating housing assistance payments. Also, six of these eight contractors should not have been granted access because there was no record of a background investigation for them. According to the TRACS management staff, contractors were granted excessive access to data and privileges because of limited staffing and the need to provide technical support to TRACS users.

Inadequate access controls increase the risk of loss of confidentiality, integrity and availability

Without adequate controls over access to TRACS, HUD is at unnecessarily increased risks of data errors and omissions, system disruptions, exploitation by unauthorized individuals for fraud and identity theft, and destruction of data by malicious hackers or disgruntled employees.

Auditee Comments

The Assistant Secretary for Housing concurred with Recommendations 1A, 1B, 1C, and 1D.

The Assistant Secretary for Administration/Chief Information Officer concurred with Recommendations 1E, 1F, and 1G, which were identified as recommendations 1F, 1G, and 1H in the draft audit report.

OIG Evaluation of Auditee Comments

We removed a redundant recommendation (number 1E in our draft report) as suggested by the Assistant Secretary for Housing. Recommendations below have been renumbered accordingly.

Recommendations

We recommend that the Assistant Secretary for Housing:

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

1B. Ensure that the TRACS Hotline Manager promptly notify the IT Operations Security Branch and all staff members who need to know about contractor and employee

job changes or employee terminations.

1C. Enforce current policies that require the Security Administrator, with assistance from the IT Operations Security Branch, to identify individuals having access to TRACS and to conduct quarterly reviews of all User-IDs issued to determine if all users still have a valid need to access resources and data at current level of privilege.

1D. Implement an automated mechanism that consolidates the different security reports.

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

1E. Ensure that the contractor's System Management Group immediately notifies the IT Operations Security Branch upon deletion of all data file sets defined within the application's Profile IDs or the removal of any system tool (e.g., the Platinum Reporting Facility).

1F. Ensure that the IT Operations Security Branch provide 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.

Inadequate Controls Over Software Configuration Management

Software configuration management⁶ controls were inadequate. We found instances of (1) noncompliance with configuration management emergency fix procedures, (2) incomplete baseline verifications, and (3) an openly revealed User ID and Password for the TRACS client server application.

Criteria

The Federal Information System Controls Audit Manual (FISCAM) published by the General Accounting Office (GAO) indicates that controls should be established over the configuration of application software programs to ensure that only authorized programs and modifications are implemented. This is accomplished by instituting policies, procedures, and techniques to ensure all software programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. FISCAM also provides that work responsibilities should be segregated so that one individual does not control all critical stages of a process. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Accordingly, system users should be granted access to only those resources they need to perform their official duties. FISCAM further states that programmers should not be responsible for moving programs into production or have access to production libraries or data. Only user, not computer staff, should be responsible for transaction origination or correction and for initiating changes to application files.

National Institute of Standards and Technology (NIST) "Principles and Practices for Securing IT Systems," in section 3.11.3, Passwords, provides that if passwords are used for authentication, organizations should teach users not to store passwords where others can find them. Section

⁶ Configuration management is the control and documentation of changes made to a system's hardware, software and documentation throughout the development and operational life of the system.

3.12.2, Access Control Mechanisms, indicates that organizations should carefully administer access control. This includes implementing, monitoring, modifying, testing, and terminating user access on the system.

Proper procedures for conducting configuration management emergency fixes are not followed

We found that contractor support personnel did not follow HUD's Configuration Management Procedures for conducting application emergency fix releases⁷, including the use of maintenance libraries. This condition exists because TRACS management did not (i) include the necessary procedures in the TRACS Configuration Management Plan; (ii) inform the contractors about the proper procedures; and (iii) did not require adherence to the configuration management emergency fix procedures.

Also, according to the Endeavor Administrator, they did not follow the proper configuration management procedures for conducting application emergency fix releases to avoid having their actions recorded. He also stated that management did not require them to follow the procedures because they are not concerned with how errors are corrected. Rather, their concern is that the system does not have downtime and that end users are satisfied.

Baseline verifications are incomplete

We found that baseline verifications are not complete to ensure synchronization of all production modules with both the Endeavor and Polytron Version Control System (PVCS)⁸ modules. The baseline verification process synchronizes all production modules with the Endeavor and PVCS modules to identify any missing, mismatched or obsolete modules, and to ensure that the current version is being used in production. Performing a baseline verification is critical for applications that utilize the CM tools such as Endeavor and PVCS. Therefore, if a baseline verification is not performed, any mismatched, missing, or obsolete modules cannot be identified if this module is not one of the modified components.

This condition occurred because development programmers did not comply with baseline verification policies as

⁷ HUD's Configuration Management Procedures, Section 3.2, explains that emergency fix release procedures are used to resolve time sensitive production application problems. These problems usually occur in applications that are being executed and they must be resolved to correct and complete the current application's execution. In general, application emergency problems are fixed within 24 hours.

⁸ HUD uses the automated CM tool called PVCS to control software changes and release for applications on the client-server and web application, and Endeavor on the IBM compatible Hitachi mainframe computers. All software changes, including emergency fixes, must go through the CM tools such as PVCS and Endeavor.

outlined in the Configuration Management Policies documentation.

A User ID and Password were openly revealed in the HARTS instruction document

We found that the HUD Application Release Tracking System (HARTS) instruction document openly reveals the Test Center's logon User-ID and Password for the TRACS client server application. This condition occurred because a standardized practice of concealing the logon User-ID or password in the HARTS instructions has not been established and enforced.

Inadequate controls over configuration management increases the risk of unauthorized changes to computer programs and data

Without adequate controls over configuration management, HUD is at unnecessarily increased risks of: (i) unauthorized changes to computer programs, (ii) inadequate testing, documentation, and approval of changes in computer programs, and (iii) unauthorized access to and distribution of computer programs. In addition, the Department risks diminishing the reliability of computerized data and increases the risk of destruction or inappropriate disclosure of data.

Auditee Comments

The Assistant Secretary for Administration/Chief Information Officer concurred with Recommendation 2A.

The Assistant Secretary for Housing partially concurred with Recommendations 2B stating that Multifamily Housing, TRACS IT Project Manager, and the Developer Contract staff already have in place strict procedures for implementing program modifications and that the TRACS Configuration Management Plan includes procedures for handling emergency fixes. Additionally, Multifamily Housing is currently working with the IT Project Manager for TRACS, the Developer Contract staff, and ADP Security on approval of a documented Production Access Plan, specifically for TRACS, for consideration as an enhancement to the current configuration management emergency fix procedures.

Housing did not state whether it concurred or non-concurred with Recommendation 2C. Rather, in response to Recommendation 2C, Housing refers to its proposed corrective action for Recommendation 2B.

OIG Evaluation of
Auditee Comments

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

Comments from the Assistant Secretary for Housing were not responsive to our findings and recommendations.

We agree with Housing's comment that the Change Control Process is identified in the Configuration Management Plan. But this process does not specifically address emergency fix procedures nor does it cover how the emergency fixes are to be made to the emergency libraries and how the changes made should be moved from the emergency libraries to the production libraries. Section 3.0 appears to cover the non-emergency fixes and does not identify the emergency fix libraries used for PVCS and Endeavor.

Regarding the comments pertaining to the Production Access Plan dated July 11, 2003, during the audit we requested that ADP Security and DPPD review and comment on the plan. Upon reviewing the plan, ADP Security provided comments stating: "Provide the developer/contractor with a file, F87.MAINT, to allow read/write/alter/delete access." DPPD provided comments stating: "The 'MAINT' library concept allows contract developers the opportunity to copy 'true Production' data and/or libraries into F87.MAINT...data files and/or libraries for modification as part of a production abend fix or corrective action plan/solution." We believe that both of these comments are clear indications that TRACS developers/contractors should utilize the emergency fix libraries under qualifier F87.MAINT for the emergency fixes. We forwarded both ADP Security's and DPPD's responses to the TRACS Government Technical Monitor (GTM) so that corrective action could be taken immediately.

We recommended development of job control language (JCL)⁹ for TRACS that would allow regular updates to the

⁹ An IBM language used to control start and execution of computer programs on a mainframe computer. As explained at search390.techtarget.com: "JCL statements mainly specify the input *data sets* (files) that must be accessed, the output data set to be created or updated, what resources must be allocated for the job, and the programs that are to run, using these input and output data sets. A set of JCL statements for a job is itself stored as a data set and can be started interactively."

maintenance library. This was because TRACS computer support staff had indicated that the modules residing in the MAINT libraries were not up-to-date and their use had been discouraged. If the batch job included regular updates of the MAINT libraries, then the TRACS developer/contractor should be able to use the MAINT libraries for emergency fixes.

As to current procedures for implementing TRACS program modifications, we agree with most procedures. However, the first one has an inherent control weakness. The control weakness is that the same personnel have been assigned to the Approval Group for different stages under Endeavor. This allows the members of the Approval Group to perform all stages of development, including testing and production functions, within the development environment. These functions should be separated to ensure integrity. In our opinion, either the Approval Group should be redefined to achieve a segregation of duties (a preventive control) or a monitoring procedure should be developed to detect and deter undesirable action.

Housing's proposed corrective action for Recommendation 2C was a reference to its corrective actions for Recommendation 2B. The corrective action for Recommendation 2B does not address how the synchronization of all production modules with both the Endeavor and PVCS modules will be conducted or when they plan to complete the synchronization. The synchronization of all production modules with both the Endeavor and PVCS is not related to ADP Security.

Recommendations

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

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.

We recommend that the Assistant Secretary for Housing:

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 Endeavor and PVCS modules.

Adequate Security Training Has Not Been Provided

Adequate security training has not been provided to HUD employees, contractor support personnel, and Internet users who are involved in the management, use, or operation of the TRACS. We found no record of (1) users' acknowledgment of the HUD security-related Rules of Behavior prior to being granted system access; (2) key system security personnel or external users being provided with adequate security training; or (3) a Memo of Understanding (MOU) between HUD and its Public Housing Authorities (PHAs) addressing each party's responsibilities for security and privacy issues.

Criteria

OMB Circular A-130 requires Federal agencies to:

- Provide appropriate training for users of Federal information resources and train personnel in skills appropriate to the management of information.
- Develop and conduct training in accordance with the Privacy Act and Computer Security Act.
 - The Privacy Act. The Privacy Act requires agencies conduct biannual reviews of its agency's training practices in order that all agency personnel are familiar with any special requirement of their specific jobs.
 - The Computer Security Act. The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of *all* employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency.
- Provide mandatory training on the rules of the system before being allowed to use the system. Each new user in some sense introduces a risk to all other users. Training reduces the risk by educating users on what constitutes acceptable behavior.

The HUD Information Resource Management Policies, Directive 24001, Chapter 3-1(n), requires that users of HUD's automated systems receive training. Chapter 2-1(i) states that training should ensure that users appropriately safeguard information resources.

The HUD Handbook 2400.24 REV-2, "Information Security Program," requires basic awareness training to be completed prior to issuance of a User-ID for a major application. Each individual indicates that the course has been completed and they have read Chapter 7 of the security Handbook when they request User-IDs and Passwords. The overall idea is to provide information needed to secure the system and minimize risk. All employee and contractors involved should be aware of the system rules before being allowed access to systems. It also requires security training to be incorporated as a part of the application security plan.

NIST SP 800-14 states that if a system has external users, its owners have a responsibility to share security measures and awareness.

Users have not acknowledged receipt of HUD security-related Rules of Behavior

We found that there is no record of TRACS users' acknowledgment of the HUD security-related Rules of Behavior prior to their being granted access to the system. Although it does not equate to actual security training, the Rules of Behavior convey and provide users with basic security awareness guidance. The Rules of Behavior are basic rules based on federal laws and regulations that are conveyed to each user and the consequences of noncompliance. They are included as part of the User Access Registration (UAR) HUD Form 22017. Each user should sign and acknowledge these rules prior to access. Unless there is an acknowledgement of those rules, there is uncertainty that users have been provided basic guidance.

Training for TRACS security personnel has not been adequate

We found that key system security personnel for TRACS have not had adequate security training. With the exception of the Departmental IT Security Awareness Training provided to all system users, the key TRACS security personnel have had either no or very limited security training. For example, the Security Administrator has not been provided with basic, intermediate, or advanced training that would equip him with the

knowledge and skills that are necessary to carry out his responsibilities as Security Administrator. According to TRACS management, adequate training has not been provided due to a lack of sufficient funding and resources.

Security training for TRACS Internet (external) users has not been provided.

We found that security training has not been provided to TRACS Internet users. For example, according to key personnel at one of the Public Housing Authorities (PHAs) we visited, personnel have not received any security training or guidance. According to key personnel at another PHA we visited, the TRACS Internet users at this site also were not provided with adequate security training. However, the IT staff at this PHA was knowledgeable about information security and had taken the initiative to develop internal security policies and procedures that are contained in their technical and security handbook. These Internet users are not casual surfers. Rather they are external users authorized by HUD to access TRACS to do their work involving HUD assistance and contract payments. Therefore, they too should be provided with security training and awareness as required by the Computer Security Act.

No Memorandums of Understanding (MOU) between HUD and its PHAs

We found no records of Memorandums of Understanding (MOU) between HUD and its PHAs. An MOU would address each party's responsibilities pertaining to security and Privacy Act requirements. It would also serve as an agreement between HUD and PHAs on the TRACS-related policies and procedures on security and technology responsibilities. An agreement could protect the agency's information, minimize its liability, protect its image, and maximize operational effectiveness. Without a clear understanding of security policies and procedures defined by an MOU, a weakness at an external partner could expose TRACS to additional vulnerabilities. For example, if one of the external sites is compromised that site could be used as a conduit to retrieve sensitive and confidential data such as tenant names and social security numbers that may have been downloaded onto a desktop computer. Printed copies of such information left in plain view or improperly disposed of could be found and used for fraudulent activity. By clearly defining security and technology responsibilities, HUD can mitigate risks from vulnerabilities at an external partner's site and reduce the agency's potential liability.

Finding 3

Inadequate security training often results in insecure systems.

Without adequate security training, users may not be aware of the system or application rules and their responsibilities. A properly trained and experienced systems security staff is essential to the security of an organization's computer network. The absence of sufficient training and adequate staffing often results in highly insecure systems. Also, poor decisions by security staff can result in system compromises, increased risk of unintentional disclosure of sensitive information, and cause damage to critical systems or data.

Auditee Comments

The Assistant Secretary for Housing concurred with Recommendations 3A and 3B.

The Assistant Secretary for Administration/Chief Information Officer concurred with Recommendation 3C.

OIG Evaluation of Auditee Comments

Comments from Assistant Secretary for Housing and the Assistant Secretary for Administration/Chief Information Officer's were responsive to our findings and recommendations.

Recommendations

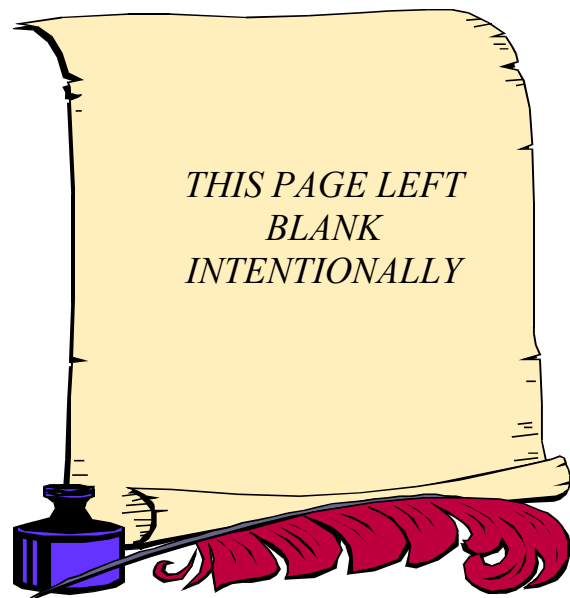
We recommend that the Assistant Secretary for Housing:

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 contractor support staff involved in the management, use, or operation of TRACS.

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.

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

3C. Ensure amendment of the User Access Registration form to include application (TRACS) users acknowledging the security-related Rules of Behavior prior to being granted system access.



Audit Logs Are Not Properly Used

We found that DB2¹⁰ system audit trail reports are neither monitored nor reviewed. We also found that TRACS security personnel do not utilize application-level audit trails to detect security violations, performance problems, transactions, and flaws in the application. Security personnel do not monitor and log user activities, including data files opened and closed, and specific actions such as reading, editing, and deleting records and printing reports.

Criteria

NIST SP 800-27, “Engineering Principles for Information Security: A Baseline for Achieving Security,” dated June 2001, Principle number 20, states that audit mechanisms to detect unauthorized use and to support incident investigations should be implemented. It further states that organizations should monitor, record and periodically review audit logs to identify unauthorized use and to ensure that system resources are functioning properly.

NIST SP 800-14, “Generally Accepted Principles and Practices for Securing Information Technology,” dated September 1996, outlines the common IT security practices that are in use today and shows what should be done to enhance or measure an existing computer security program or to aid in the development of a new program. It identifies practices that provide a common ground for determining the security of an organization. It specifically, states that audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can and should be used to provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. It further states that audit trail records should include sufficient information to establish what events occurred and who or what caused them. In general, an event record should specify the type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event. The audit trails should also be

¹⁰ DB2 is a database management system. It is important because it plays an integral part in the administration of an application’s data. Additionally, it organizes data and can offer some level of security over access to a system’s information and resources.

DB2 system audit reports are not monitored or reviewed

protected from unauthorized access and reviewed periodically for any unusual or unauthorized activities.

DB2 is IBM's database management software that organizes TRACS data. It also provides its own access control over TRACS. One of the features that DB2 offers is a log of all transactions and resources used by a given application. This feature is called the audit trail. We found that although the DB2 system audit trail feature had been turned on, no one was monitoring or reviewing the audit reports generated as a result of this feature. This condition occurred because there was no clear guidance specifying who is responsible for monitoring and reviewing security violations recorded in the DB2 system audit report. Turning on the audit trail feature serves no useful purpose if the reports generated are not reviewed.

No audit trails at the application-level

We also found that TRACS security personnel do not utilize application-level audit trails to detect security violations, performance problems, transactions, and flaws in the application or monitor and log user activities. There were no application-level audit trails because management was not using the audit logs for its intended purpose. Management misunderstood the purpose of the audit logs and incorrectly used them to track tenant certifications rather than identify security violations and performance problems. TRACS management and security personnel confirmed that the audit trail is not used.

Unauthorized activities can't be detected and investigated if audit logs are not used properly

Without an audit log to monitor user activities, the Department is unable to record and detect any unauthorized activities. Evidence for investigation and prosecution of unlawful intrusions is lost.

Auditee Comments

The Assistant Secretary for Housing concurs with the recommendation to enforce the usage and periodic review of the audit logs. However, Housing took exception to the finding and was not clear about why its non-technical staff would be assigned the responsibility of extracting data from and interpreting DB2 audit logs.

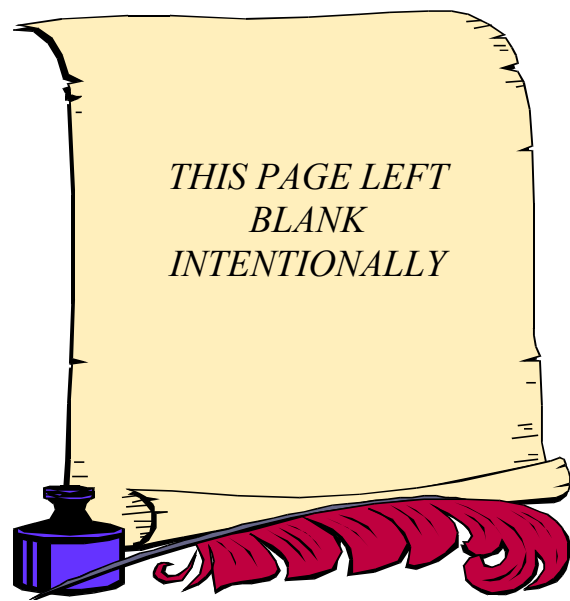
OIG Evaluation of Auditee Comments

Comments from the Assistant Secretary for Housing were responsive to our findings and recommendation.

Recommendations

We recommend that the Assistant Secretary for Housing:

4A. Enforce the usage 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.



Weak Personnel Security Practices Continue to Pose Risks of Unauthorized Access to TRACS

For several years we have reported that HUD's personnel security practices for access to critical and sensitive systems has been inadequate. Although HUD has made progress in addressing reported problems, risks of unauthorized access to the Department's critical financial systems remains a major concern. During this audit, we found 37 users out of a total of 870 users who were given greater-than-read access to TRACS without a record of an appropriate background investigation.

Criteria

OMB Circular A-130, Appendix III, provides that agency programs shall include certain controls in their general support systems and major application systems. Specifically, personnel controls shall include controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate. In cases where such controls cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to access the application and periodically thereafter.

According to HUD Handbook 2400.24 REV-2, "Information Security Program," dated November 10, 1999, Chapter 4, Section 4-4.i, 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." Section 4-2.b.2 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." Section 4-2.b.7, states that the Security Administrator of a major application system is responsible for communicating the requirement for individuals to submit background investigation forms based on their

information system related functions. Section 4-10.i., states that the Office of Human Resources (OHR) shall obtain employee and contractor background investigation forms from System Owners, Security Administrators or Government Technical Representative. Appendix J, "Background Investigations," Section J-1, "Screening of Personnel," states that screening of Federal employees is required by Executive Order 10450 (Security Requirements for Government Employment), 5 CFR Title 5, Code of Federal Regulations. Most HUD employees receive at least a National Agency Check and Inquiries (NACI).

Written policy is not being followed

We found that inappropriate access to TRACS was granted because the policy requiring users who request greater-than-read access to HUD's sensitive systems to submit proper system access forms was not being adhered to. In November 2000, the OCIO issued a memorandum establishing new user registration procedures for IT systems access. These procedures required HUD employees and HUD contractors to use the User Access Registration (UAR) form (HUD Form 22017) for requesting access to HUD's systems. The UAR form was updated to include the Office of Security and Emergency Planning (OSEP) in this process to ensure that users accessing HUD's sensitive and critical systems had the appropriate background investigation. However, during our review we found that there were users who had not been certified by OSEP because the TRACS System Administrator was not submitting the HUD Form 22017 to OSEP prior to upgrading users' access privileges.

Lack of coordination between TRACS System Administrator, IT Operations Security Branch, and OSEP

We also found that HUD has system access procedures in place. Nonetheless, inappropriate access to TRACS was granted because 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 more than read-only access privileges. For example, to upgrade a user's access privileges from read-only to greater-than-read, a UAR should be forwarded to OSEP to determine whether the user has had a background investigation and to the IT Operations Security Branch. However, the System Administrator bypassed established system access procedures and upgraded the access privileges of 7 of the 37 users without background investigations. IT Security

was not aware of the upgraded access privileges from its original grant of read-only access privileges.

No central repository to track all users' access levels

Additionally, we found that inappropriate access to TRACS was granted because the IT Operations Security Branch does not have a central repository that would serve as a master inventory tracking system to identify users with above read access at the application level. There is no mechanism 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. This further hampers the Department's ability to conduct accurate reconciliations on a periodic (at least quarterly) basis since we cannot be assured that the access security data being provided is accurate and complete.

Inadequate personnel security controls increase the risk of loss of data confidentiality, integrity, and availability

Without adequate personnel security controls, unauthorized users could have access to sensitive and critical data and may compromise the confidentiality, integrity, and availability of critical and sensitive data.

Auditee Comments

The Assistant Secretary for Administration/Chief Information Officer concurred with Recommendations 5A and 5B.

The Assistant Secretary for Housing concurred with Recommendation 5C.

OIG Evaluation of Auditee Comments

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

Recommendations

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

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.

We recommend that the Assistant Secretary for Housing:

5C. Ensure implementation of an automated system or mechanism that would require the TRACS Security Administrator to coordinate with IT Security and Personnel Security prior to granting a user above-read access privileges.

Key Personnel Lack Segregation of Duties

We found several instances where the key duties and responsibilities of the TRACS Security Administrator, Database Administrator, and Technical Lead were not adequately separated. This gives him the ability to authorize users and update data and financial transactions.

We also found that the TRACS DB2 Database Administrator is also performing two other, incompatible functions. Also, we found that there are contractor support personnel who can simultaneously conduct development, testing, and production functions within the development environment. Additionally, we found that a contractor employed as a computer programmer was granted excessive access privileges in order to perform manual interventions for the batch job process.

Criteria

OMB Circular A-123 states that key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions should be separated among individuals. Managers should exercise appropriate oversight to ensure individuals do not exceed or abuse their assigned authorities.

Federal Information Processing Standard (FIPS) Publication 73, published by the National Institute for Standards and Technology (NIST), states in section 7.2.2 that 'separation of duties' should be the assignment of each function, to the extent possible, to different individuals. It also states that it is important to define each function clearly so that there will be no overlap in responsibility from one function to another.

The TRACS Security Administrator is also the Data Base Administrator and Technical Lead

Key duties and responsibilities among the TRACS security personnel were not adequately segregated. Specifically, the Security Administrator is also functioning as both the Data Base Administrator for TRACS and the Technical Lead. This gives him the ability to authorize users access and update data and financial transactions.

Lack of segregation of duties among contractor support personnel

We found several instances where contractor support personnel functions were not adequately separated. Specifically, we found that there are contractors who can simultaneously conducting development, testing, and production functions within the development environment. This lack of segregation of duties does not allow for

assurance that all software programs and program modifications are properly authorized, tested, and approved. Nor does it provide assurance that one individual does not control all critical stages of a process.

We also found that the TRACS DB2 Database Administrator is also performing other, incompatible functions. Specifically, the TRACS DB2 Database Administrator is also the CoolGen Administrator¹¹ and has the ability to conduct development, testing, and production functions within the development environment. According to the Endeavor Administrator, there has been a lack of sufficient personnel to separately support these three functions. Consequently, reliance to perform these duties and responsibilities were placed on the same individuals.

Additionally, we found that a contractor employed as a computer programmer was granted excessive access privileges in order to perform manual interventions for the batch job process. For example, when a batch job is submitted, sometimes the job may have errors that would normally be detected by an edit check feature built into the system. However, in this case, a sufficient edit check or automated data error correction feature was not designed into the system and therefore, manual interventions were necessary to correct the problem.



Auditee Comments

The Assistant Secretary for Housing partially concurred with Recommendation 6A. Housing concurred that qualified staff are needed to support security functions.

Housing did not concur with the recommendation that technical support responsibilities and security-related tasks be 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 Endeavor environment, and (2) TRACS DB2 Database Administrator, Endeavor approver group, and CoolGen Administrator.

¹¹ The CoolGen Administrator is the person who manages CoolGen, one of the software tools that HUD uses to support configuration management activities in both the mainframe and client-server environments.

Housing disagreed with our finding that “the Security Administrator is also functioning as both the Data Base Administrator for TRACS and the Technical Lead. This gives him the ability to authorize users access and update data and financial transactions.” Housing stated that this is not an accurate statement and it should be removed. Housing further stated that the Security Administrator is not a Database Administrator (DBA) and that the TRACS Security Administrator position is staffed by the Office of Housing. The TRACS DBA is staffed by the TRACS support contractor. Similarly, the technical lead is also staffed by the TRACS support contractor. Each of these positions is filled by a different person.

Housing also disagreed with our finding that “we found that there are contractors who are simultaneously conducting development, testing, and production functions within the development environment.” According to Housing, this statement is inaccurate and should be removed. Housing further states that there is a segregation of duties and responsibilities between development, testing, and production functions.

Regarding our finding that “We also found that the TRACS DB2 Database Administrator is also performing other, incompatible functions. Specifically, the TRACS DB2 Database Administrator is also the Cool:Gen Administrator...,” Housing was unclear as to why a separation of development DBA tasks and development Cool:Gen duties is required.

Housing did not state whether it concurred or non-concurred with Recommendation 6B. Housing stated that the actions by TRACS personnel for supporting batch transaction updates are identified in Section 1.3.2 of the TRACS Production Access Plan. Housing also stated that a batch update process is in place to detect and reject erroneous data and that user data not conforming to TRACS requirements are rejected, and automated messages are sent to the User to correct and resubmit. Housing stated that when required, the TRACS Production Control Staff performs a batch process that can remove incorrectly formatted transactions that cause job failures or cause the overnight process to not be completed by 7:00 am the following morning.

OIG Evaluation of
Auditee Comments

Comments from the Assistant Secretary for Housing were not responsive to our findings and recommendations.

We agree with the comment that the Security Administrator is not a Database Administrator nor Technical Lead. However, based on our interview with the then Security Administrator, he provided technical support to end users and performed functions that the TRACS Security Application Plan defined as Database Administrator functions (i.e., establishes and maintains inventory of functions that are used to add, delete, or change system records in TRACS and assigns and monitors functional access privileges). We maintain that these functional areas should be segregated and the Security Administrator should not function in a technical support role. In addition, his role provided him with functional access to ARAMS. Based on our review of his access to the ARAMS module, this gave him the ability to update and delete records and reference tables and the ability to promote renewal reservations from IN Clearance to Approved status.

As suggested, we revised the statement in our draft report that “we found that there are contractors who are simultaneously conducting development, testing, and production functions within the development environment.” To be accurate, we stated “we found that there are contractors who *can* simultaneously conduct development, testing, and production functions within the development environment.” Again, as stated in our response to Housing’s comments on recommendation 2B, the same personnel have been assigned to the Approval Group for different stages under Endeavor. This has provided opportunities for the members of the Approval Group to perform all of the stages of development, testing and production functions within the development environment. In our opinion, TRACS management should either redefine the Approval Group or develop a monitoring procedure to minimize the risk of simultaneous development, testing, and production functions actually being performed.

In response to Housing’s uncertainty as to why a separation of development DBA tasks and development Cool:Gen duties is required, we iterate that according to the GAO

FISCAM, work responsibilities should be segregated so that one individual does not control all critical stages of a process. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. 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.

During our audit, we discussed with Housing Program officials our finding that a contractor employed as a development computer programmer had been granted excessive access privileges to the TRACS production batch job process. We expressed our opinion that this was a weakness in internal control and recommended that the programmer's access to production be reduced to read only. Program officials explained that the programmer's ability to change production software coding and data were required in order for him to correct data errors that caused interruptions in the production batch job. Consequently, in our discussions with program officials and later in our draft report we recommended development of an edit routine to check data before passing it to the production job. This would eliminate the stated need for the programmer's excessive production access privileges. In commenting on this recommendation (number 6B) in our draft report, Housing stated that "a batch process is in place to detect and reject erroneous data." After receiving this comment, we requested the source code and JCL for the process to verify its existence. We also requested the Production Control Problem Log to examine the history of the programmer's intervention in the production batch job process. Housing program officials did not provide us with the source code and JCL for the edit routine so we were unable to verify its existence. Comments provided with the transmittal of the Production Control Problem Log suggest that there are no edit routines outside of the production batch process. The Production Control Problem Log provided to us shows that "since implementation of the log started last year" there were only 8 instances when the programmer was asked to resolve problems. None of the problems were related to data errors. Six of the eight problems pertained to message processing issues with

TRACSMail. It appears that the message processing problem has existed for at least a year. Apparently, the TRACS team did not identify the cause of the problem and resolve it (eliminating the need for manual intervention.). Considering this information, we revised our recommendation. We now recommend that the programmer's production access be reduced to read-only and that emergency fix procedures be followed when his intervention is required.

Recommendations

We recommend that the Assistant Secretary for Housing:

6A. Ensure that the Office of Multi-family Housing has the necessary resources 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 Endeavor environment, and (2) TRACS DB2 Database Administrator, Endeavor approver group, and CoolGen Administrator.

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

Auditee Comments



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

OFFICE OF THE ASSISTANT SECRETARY
FOR HOUSING-FEDERAL HOUSING COMMISSIONER

COPY

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

FROM: 
John C. Weicher, Assistant Secretary for Housing- Federal Housing
Commissioner, H

SUBJECT: Draft Audit Report on Application Control Review of the Tenant Rental
Assistance Certification System (TRACS)

Office of Inspector General (OIG) audit 2004-DP-XXXX contains six findings with recommendations requiring action by the Office of Housing and the Office of Administration/Office of the Chief Information Officer. The findings address:

- Inadequate access controls over the TRACS data and resources,
- Inadequate controls over software configuration management,
- Lack of security training,
- Inadequate review of audit logs to detect security violations, performance problems, or to monitor and log user activities,
Weak personnel security practices, and
Lack of segregation of duties.

The Office of Housing's responses to the Tenant Rental Assistance Certification System (TRACS) audit recommendations are provided below. If you disagree with our responses, please let us know as soon as possible so we can provide any additional information needed or discuss possible compromises.

The OIG recommends the Assistant Secretary for Housing improve/provide the following controls:

1. Access Controls Over TRACS Data and Resources are Inadequate

Recommendation 1A: Enforce current policies requiring system owners, with the assistance of its program supervisors and Security Administrators, to ensure that system access is based on the need to perform specific job functions.

The Office of Housing concurs. Multifamily Housing is taking several steps to ensure that TRACS users actually require systems access to do their jobs. The TRACS Rules of Behavior have been included with the TRACS User Access Form, and plans are underway to implement Hub/Program Center Level Security Administrators who will work directly with Program

www.hud.gov

espanol.hud.gov

supervisors in their respective areas in ensuring that supervisors are accountable for system access based on specific job functions. The Hub Level Security Administrators will work directly with the Headquarters Security Administrator for TRACS.

Corrective Actions	Target Date	Documentary Evidence
Ensure Rules of Behavior are signed by all users requesting access to TRACS and implement Multifamily Hub-level Security Administrators.	Partially completed. Final Implementation: March 2004	Signed copies of User Access Forms and Rules of Behavior for TRACS; Signed Memorandum of Understanding or DAS directive regarding MF Hub-Level Security Administrators.

Recommendation 1B: Ensure that the TRACS Hotline Manager promptly notifies the IT Operations Security Branch and all staff members who need to know about contractor and employee job changes or employee terminations.

The Office of Housing concurs. A report of all contractor staff for the TRACS Hotline Manager will be included when defining requirements for database changes and new system functionality.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> ▪ Prepare and issue a user listing of all contractors with access to TRACS for distribution to the TRACS Hotline Manager with Quarterly user reviews. 	Ongoing; first implementation March 2004	User listings issued during March 2004 Quarterly Review

Recommendation 1C: Enforce current policies that require the Security Administrator, with assistance from the IT Operations Security Branch, to identify individuals having access to TRACS and to conduct quarterly reviews of all User-IDs issued to determine if all users still have a valid need to access resources and data at current level of privilege.

The Office of Housing concurs. Multifamily Housing will prepare a user certification document to be issued during quarterly reviews of all users with access to TRACS. A user access list identifying all users in a given Multifamily field office will be provided to the respective Multifamily offices. Plans are underway to implement Hub/Program Center Level Security Administrators who will work directly with Program supervisors in their respective areas in ensuring supervisor accountability for system access based on consistency between job functions and levels of access privilege. The Hub Level Security Administrators will work directly with the Headquarters Security Administrator for TRACS.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> ▪ Maintain and distribute an updated TRACS User Access list to be issued 	March 2004	User listings to be issued during March 2004 Quarterly

on a quarterly basis for certifying user access privileges.		Review
<ul style="list-style-type: none"> ■ Develop and distribute a user certification document to be issued along with the User Access List quarterly. 	March 2004	User listings and certification document issued during March 2004 Quarterly Review
<ul style="list-style-type: none"> ■ Implement Multifamily Hub level Security Administrators. 	Partially completed. Final Implementation: March 2004	Signed Memorandum of Understanding or Deputy Assistant Secretary for Multifamily Housing directive regarding MF Hub level Security Administrators.

Recommendation 1D: Implement an automated mechanism that consolidates the different security reports.

The Office of Housing concurs. Multifamily Housing has already implemented a relational database system to identify and maintain all Intranet and Internet users to TRACS along with their application level access privileges (with help from the WASS team). The database has been in place since January 2003. We will also work with the ADP Security and the TRACS Team to include more files and tables, further identifying mainframe users and application level access.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> ■ Incorporate data files from the mainframe to further identify users and their access privileges, sources of data TRACS Team and ADP Security. 	Ongoing	Database System
<ul style="list-style-type: none"> ■ MFH has submitted a request to OMB to enhance the security modules within the TRACS mainframe and Intranet systems. 	To Be Determined	OMB 300 FY 2003 Submission

Recommendation 1E: Enforce current policies that require the Security Administrator, with assistance from the IT Operations Security Branch, to conduct quarterly reviews of all User-IDs issued to determine if all users still have a valid need to access resources and data at current level of privilege.

This recommendation is redundant and should be deleted. It is fully incorporated in Recommendation 1C.

2. Controls Over Configuration Management are Inadequate

Two statements on page 10 should be revised or removed:

- On page 10, second paragraph, a reference is made that contractor support personnel do not follow HUD’s CM procedures for conducting application emergency fix releases. It was further explained that this was because the TRACS CM Plan did not document this process. This statement is not accurate. In Section 3.0 (Change Control Process) of the TRACS CM Plan (July 2003) there is a description of the contractor’s tasks in using a change request form and identifying the severity levels associated with the ER. The TRACS staff are familiar with this process and use this for ERs.
- On page 10, third paragraph, the audit states, “according to the Endeavor Administrator, they (TRACS Team) did not follow the proper configuration management procedures for conducting application emergency fix releases to avoid having their actions recorded.” The implications suggest an unprofessional if not fraudulent desire to subvert management reviews. If this is not the intention of the auditor, the statement should be reworded.

If the audit intends to identify a specific problem, the audit’s findings should directly address this very serious comment. Housing recommends that unless a finding is going to directly address subversion and provide a justification beyond a 3rd party opinion, the unsubstantiated statement should be removed.

Recommendation 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.

Housing does not fully concur with this finding and recommendation. Multifamily Housing, TRACS IT Project Manager, and the Developer Contract staff already have in place strict procedures for implementing program modifications. The TRACS Configuration Management Plan includes procedures for handling emergency fixes. Additionally, Multifamily Housing is currently working with the IT Project Manager for TRACS, the Developer Contract staff, and ADP Security on approval of a documented Production Access Plan, specifically for TRACS, for consideration as an enhancement to the current configuration management emergency fix procedures.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> ■ Submit a Production Access Plan to ADP Security for incorporation into the current Configuration Management Plan that addresses the specific needs of TRACS. 	Pending ADP Security approval	Written Production Access Plan incorporated in Configuration Management Plan

TRACS current procedures for implementing program modifications:

TRACS Endeavor development programmer does not conduct development, testing, and production functions within the development environment

- Change Requests - formal request documenting the need for a system modification
- System Specifications - describe, in detail, any required program modifications
- Unit Testing - developer assigned to code program modification, tests the changes
- System Testing - TRACS test team, test program modification
- Migration Forms - completed and submitted for migrating program modification from one region to another (unit test -> system test -> production)
- Updates to the Batch Operations Manual (if required)
QA of procedure once implemented

NOTE: All of these steps are described in detail in the TRACS Configuration Management Plan. The Configuration Management Policy applies to software only and does not include data files.

Recommendation 2C: Ensure that the TRACS system owner include the procedures and policies 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 Endeavor and PVCS modules.

Corrective Actions	Target Date	Documentary Evidence
▪ Refer to Housing Response to Recommendation #2B for Corrective Actions	See Rec. #2B	N/A

3. Adequate Security Training Has Not Been Provided

Recommendation 3A. Ensure that adequate resources are available for implementation of mandatory and periodic systems-specific security training for all individuals, including but not limited to the system owner, Systems Security Officer, HUD Employees, and TRACS contractor support staff involved in the management, use, or operation of the TRACS.

Housing concurs that HUD staff should get adequate training on TRACS. Ability to conduct the training, however, depends on availability of training funds. Multifamily Housing has received special funding this year for a training initiative and is in the process of procuring resources and staff to assist with the preparation of training plans and materials.

Corrective Action	Target Date	Documentary Evidence
MFH has submitted procurement requests for system-specific training over the next two years including, but not limited to, training on security and other topics for all users including Security Systems Administrator.	Pending DAS approval	Copies of CMRB Request and Approval forms

Recommendation 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.

Housing concurs and will develop a plan and schedule to work with the CIO's Office to address the establishment of MOUs with the Internet Users, i.e. Housing Authorities, Contract Administrators, etc.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> MFH has prepared a TRACS Security Transition plan and will include as an action item, recommendation #3B. 	Pending Management Approval	TRACS Security Transition Plan document

4. Audit Logs are Not Properly Used

Recommendation 4: Enforce the usage 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.

This finding should be modified by the OIG to consider the following:

The OIG fails to identify specific control metrics the Office of Housing is to extract from the DB2 audit logs. The OIG should specify the process by which it intends for the Office of Housing personnel to extract data from these logs. DB2 audit logs are not usually used by non-technical persons, and it is not clear why the audit assigns this responsibility to Housing staff to interpret these logs.

- Data files "opened" and "closed" are the result of imbedded software logic, and are not directly controlled by Housing personnel. Tracking "opening" files will probably not be insightful to Housing personnel. It is suggested that window/page options that are associated with specific types of updates be tracked.

Housing concurs with usage and periodic review of the audit logs. Since systems enhancements are needed to serve this purpose, Multifamily Housing has submitted a request to OMB for enhancements to incorporated system-level audit trails for all TRACS modules. The ARAMS module within TRACS already has audit trails incorporated.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> MFH has submitted an IT Request to OMB for enhancements to TRACS that will address incorporation of application-level audit trails and history tracking and overall security improvements. 	Pending OMB approval	OMB 300 FY 2003 Submission

5. Weak Personnel Security Practices Continue to Pose Risks of Unauthorized Access to TRACS.

Recommendation 5C: Ensure implementation of an automated system or mechanism that would require the TRACS Security Administrator to coordinate with IT Security and Personnel Security prior to granting a user above-read access privileges.

The Office of Housing concurs with the finding. Multifamily Housing has already implemented a relational database system to identify and maintain all Intranet and Internet users of TRACS along with their application level access privileges (with help from the WASS team). We will also work with the ADP Security and the TRACS Team to incorporate more files and tables, further identifying mainframe users and application level access. Finally, procedures will be developed to ensure that the TRACS Security Administrator coordinates with IT Security and Personnel Security prior to granting users above-read access privileges.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> ▪ Incorporate data files from the mainframe to further identify users and their access privileges, sources of data TRACS Team and ADP Security. 	Ongoing	Database System
<ul style="list-style-type: none"> ▪ MFH has submitted a request to OMB to enhance the security modules within the TRACS mainframe and Intranet systems. 	To Be Determined	OMB 300 FY 2003 Submission

6. Key Personnel Lack Segregation of Duties

Recommendation 6A: Ensure that the Office of Multifamily Housing has the necessary resources 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 to include proper segregation of duties and responsibilities between the (1) development, testing, and production functions within the Endeavor environment, and (2) TRACS DB2 Database Administrator, Endeavor approver group, and CoolGen Administrator.

On page 25, fifth paragraph, the audit report states that, "the Security Administrator is also functioning as both the Data Base Administrator for TRACS and the Technical Lead. This gives him the ability to authorize users access and update data and financial transactions." This is not an accurate statement and it should be removed. The Security Administrator is not a Database Administrator (DBA). The TRACS Security Administrator position is staffed by the Office of Housing. The TRACS DBA is staffed by the TRACS support contractor. Similarly, the technical lead is also staffed by the TRACS support contractor. Each of these positions is filled by a different person.

On page 25, the audit report states, “we found that there are contractors who are simultaneously conducting development, testing, and production functions within the development environment.” This statement is also inaccurate and should be removed. There is a segregation of duties and responsibilities between development, testing, and production functions. Developers perform code development and perform unit testing in the TRACS Development Region. A separate group within the TRACS staff performs systems testing.

On page 26 of the report, the OIG states, “We also found that the TRACS DB2 Database Administrator is also performing other, incompatible functions. Specifically, the TRACS DB2 Database Administrator is also the Cool:Gen Administrator” Separation of duties should be part of the quality control procedures for a given contractor. The primary goal of a separation of duties is to ensure that code development personnel do not release software into production and that they do not have access to the production database. It is unclear why a separation of development DBA tasks and development Cool:Gen duties is required.

Housing concurs that qualified staff to support security functions are needed. Multifamily Housing has submitted requests for more staff resources for the past few years and continues to request staff resources to adequately address division of duties as it relates to TRACS. The Office of Multifamily Housing has already reassigned TRACS Security Administration duties and has begun official transition, with completion expected in six months. However, Multifamily Housing has not been allowed the proper funding to provide for one individual to support each of the cited functional areas.

The duties involved with these functions do not fully constitute three (3) full-time positions. There is a segregation of duties and responsibilities between development, testing, and production functions.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> MFH has reassigned the TRACS Security Administrator duties and functions to other appropriate staff and has incorporated automated applications to track and monitor user access to TRACS. 	Completed	TRACS Security Transition Plan document and TRACS Security Plan, dated September 2003.
<ul style="list-style-type: none"> MFH is requesting funds for enhanced security training as it relates to the mainframe. MFH will work with the ADP Security office in identifying appropriate training needs for Security Administrators. 	To Be Determined	TRACS Security Transition Plan document.
<ul style="list-style-type: none"> DB2, Endeavor, and CoolGen Administrator improper segregation of duties has been addressed. 	ASAP	N/A

Recommendation 6B. Implement an automated batch job process for correcting data errors, thereby preventing the need to contract support personnel with excessive privileges to TRACS production data files.

The actions by TRACS personnel for supporting batch transaction updates are identified in Section 1.3.2 of the TRACS Production Access Plan. A batch update process is in place to detect and reject erroneous data. User data not conforming to TRACS requirements are rejected, and automated messages are sent to the User to correct and resubmit. When required, the TRACS Production Control Staff performs a batch process that can remove incorrectly formatted transactions that cause job failures or cause the overnight process to not be completed by 7:00 am the following morning.

Emergency actions taken by the TRACS production control specialist are documented and reported to the TRACS project manager, who forwards that information to the TRACS program area sponsor, who forwards the information to ADP Security.

Multifamily Housing will identify opportunities to include automated data error correction procedures when defining requirements for database changes and new system functionality. A report of all contractor staff for the TRACS Hotline Manager will also be included.

Corrective Actions	Target Date	Documentary Evidence
<ul style="list-style-type: none"> ▪ Identify appropriate automated data error correction procedures when defining system changes and/or enhancements. 	Dates of TRACS releases	Functional Requirements Documents
<ul style="list-style-type: none"> ▪ Prepare and issue a user listing of all contractors with access to TRACS to distribute to the TRACS Hotline Manager with Quarterly user reviews. 	Ongoing; first implementation March 2004	User listings issued during December 2003 Quarterly Review
<ul style="list-style-type: none"> ▪ TRACS has planned enhancements to its ARAMS module for automating many of its manual batch processes. 	ARAMS Release Schedule	Functional Requirements Document


If you have any questions or require additional information, please contact Lanier Hylton, Director, Office of Housing Assistance Contract Administration Oversight in the Office of Multifamily Housing Programs. His telephone number is (202) 708-0614, extension 2510.



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

ASSISTANT SECRETARY FOR
ADMINISTRATION/CHIEF INFORMATION OFFICER

JAN 30 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 –
Application Review of the Tenant Rental Assistance Certification
System (TRACS)

This responds to the above-referenced draft audit report, dated December 30, 2003. We concur with all recommendations in the report. There are 20 recommendations in the report of which seven are addressed to me. Please find attached the responses to those recommendations.

If you need additional information or have questions, please contact Mary Barry, Director, Office of Management and Planning, at (202) 708-1027, extension 123.

Attachment

cc:
John C. Weicher, Assistant Secretary for Housing, Federal Housing Commissioner, H

www.hud.gov espanol.hud.gov

**Office of Administration/CIO Response to OIG Draft Audit Report
Application Control Review of the Tenant Rental Assistance Certification System
(TRACS)
Dated December 30, 2003**

Recommendation 1F: Ensure that the contractor's System Management Group immediately notifies the IT Operations Security Branch upon deletion of all data file sets defined within the application's Profile IDs or the removal of any system tool (e.g., the Platinum Reporting Facility).

Response: Concur. The obsolete TRACS dataset references that were identified by the auditor have been deleted. The TRACS Database Administrator (DBA) will be tasked to notify the IT Operations Security Branch when production datasets are to be deleted from the TRACS Profile IDs. The TRACS DBA will request each month a report from the IT Departmental Platforms and Processing Division to allow assessing dataset access and system utilization. TRACS datasets that have not been referenced within the last 90 days will be a selection criterion.

A quarterly review of the TRACS Profile IDs will be conducted to determine if the TRACS datasets that have been identified as inactive are contained within the profile. The Office of ADP Security will provide the access control lists (ACL) profile reports for this periodic review. The TRACS DBA will perform the review based on the content of the ACL profile reports and by comparing them to the files identified as being obsolete. The DBA will prepare a report for the HUD TRACS Project Leader and the IT Operations Security Branch regarding analysis performed and defining actions required.

We will implement the new procedures above immediately.

Recommendation 1G: Ensure that the IT Operations Security Branch provide the TRACS Security Administrator with the appropriate user ACLs.

Response: Concur. We will begin providing the TRACS Security Administrator with the appropriate user ACLs immediately.

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

Response: Concur. All development personnel who leave the TRACS project will have their access and User IDs revoked by the TRACS Project Manager who will notify the TRACS Security Administrator who in turn will notify the IT Operations Security Branch. We will notify all personnel involved in this process and begin implementation immediately.

Recommendation 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.

Response: Concur. The procedures to address this recommendation and the estimated completion date will be detailed in our Corrective Action Plan.

Recommendation 3C: Ensure amendment of the User Access Registration form to include application (TRACS) users acknowledging the security-related Rules of Behavior prior to being granted system access.

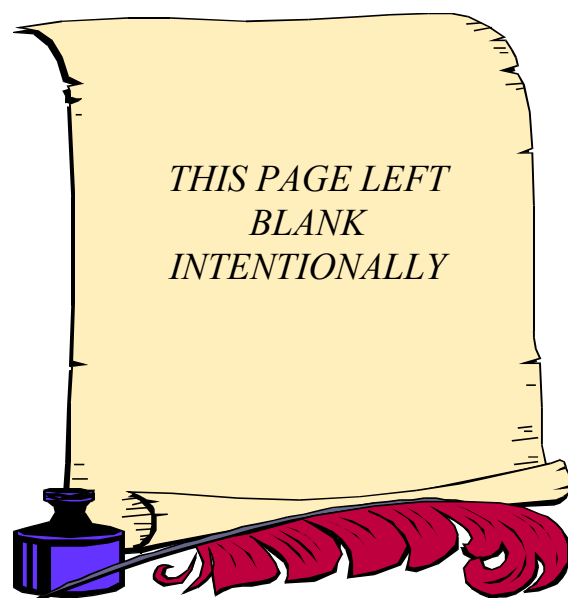
Response: Concur. We will amend the user registration form to include a reference to the Rules of Behavior for Application Systems. We will provide the estimated completion date in our Corrective Action Plan.

Recommendation 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.

Response: Concur. All personnel who have or request to have above read access to HUD's mission-critical and sensitive systems are required to submit background investigation forms. Contracts must address this requirement. We have confirmed that the TRACS support contract (C-OPC-18462) was modified in September 2003 to address the need of staff to complete these forms. We will begin immediately ensuring that this policy is followed.

Recommendation 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.

Response: Concur. The implementation of a central repository and the estimated completion date will be detailed in our Corrective Action Plan.



Distribution

The Honorable Susan M. Collins, Chairman, Committee on Government Affairs
172 Russell Senate Office Building, Washington, DC 20510

The Honorable Thomas M. Davis, III, Chairman, Committee on Government Reform
2348 Rayburn Building, House of Representatives, Washington, DC 20515-4611

The Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform
2204 Rayburn Building, House of Representatives, Washington, DC 20515

