# AUDIT REPORT


## HUD ENTITY-WIDE SECURITY PROGRAM

01-DP-166-0001

October 31, 2000

INFORMATION SYSTEMS AUDIT DIVISION
OFFICE OF AUDIT

audit report

| Issue Date |
| --- |
| October 31, 2000 |
| Audit Case Number |
| 01-DP-166-0001 |

**TO:** Saul Ramirez, Deputy Secretary, SD

**FROM:** Benjamin K. Hsiao, Director, Information Systems Audit Division, GAA

**SUBJECT:** Final Audit Report on HUD's Entity-wide Security Program

We completed an audit of HUD's entity-wide security program for computer based systems. Specifically, we evaluated whether HUD's security planning and management practices include: (1) assessing and managing risk; (2) developing and implementing effective security policies and procedures; and (3) monitoring the effectiveness of those procedures. We also reviewed the adequacy of the Department's efforts to implement Presidential Decision Directive No. 63. This Directive requires Federal entities to protect their critical infrastructures from intentional acts.

Our audit concluded that HUD's security program needs significant improvement. We found that computer security weaknesses continue to pose risks to sensitive data and critical computer resources. Numerous deficiencies noted during our review are long-standing, having been identified in previous audits and reviews. HUD has not placed the appropriate emphasis on information systems security. Our report contains a number of recommendations to strengthen information security at HUD.

Within 60 days, please submit for each recommendation a status report on: (1) corrective action taken; (2) the proposed corrective action and target completion dates; or (3) why corrective action is considered unnecessary.

We appreciate the courtesies extended to the audit staff. Questions or requests for additional information should be directed to me at (202) 708-3444, extension 149.

Attachment

# Executive Summary

Computer based information systems are crucial to all aspects of HUD's operations. HUD processes over $31.5 billion worth of transactions through HUD's Central Accounting and Program System, and the Line of Credit Control System. HUD provides funding to a broad range of grant recipients throughout the country, as well as rent and operating subsidies. These subsidies benefit over 4 million lower income households through a variety of programs, including Public Housing and Section 8. HUD also insures over $500 billion worth of both single and multifamily properties. In addition, many of HUD's data systems contain personal privacy and sensitive financial data.

We reviewed HUD's efforts to develop an entity-wide security program. During our review, we determined whether HUD has followed industry-accepted practices for an effective information security program to include: (1) assessing and managing risk; (2) developing and implementing effective security policies and procedures; and (3) monitoring the effectiveness of those procedures. We also determined the adequacy of initial planning and assessment activities undertaken to comply with Presidential Decision Directive (PDD) No. 63. PDD 63 calls for a national effort to assure the security of the nation's critical infrastructures, especially our computer based systems. By May 22, 2003, affected agencies are required to eliminate any significant vulnerability and to achieve and maintain the ability to protect its critical infrastructures from intentional acts.

During our review, we noted that HUD recently took steps to improve its security stance by implementing a network access monitoring tool called "RealSecure." However, this is only a beginning. Our review indicates that the entity-wide security program needs strengthening. Specifically, we found that: (1) risks are not adequately assessed and managed on a continuing basis; (2) security plans are either not documented or not kept current; (3) incident tracking, reporting, and response capability needs improvement; (4) an effective training and awareness program is not in place, and (5) HUD's Critical Infrastructure Protection Plan prepared in accordance with PDD 63 is inadequate and out of date. These weaknesses continue to expose HUD's critical information resources to accidental or intentional loss or damage.

Currently, responsibility and accountability for information security within the Department is fragmented and decentralized. In addition, HUD has not placed sufficient priority nor devoted adequate resources toward establishing an effective security program. As a result, HUD's capability to take corrective actions against internal or external attacks such as unauthorized access, data compromise, denial of service, and system damage is severely limited.

Since the Chief Information Officer (CIO) reports directly to the Secretary, it is in the best position to provide the necessary leadership, oversight, and enforcement for information security. We recommend that the Secretary assign the CIO full responsibility and accountability for information security and allocate adequate resources to establish an effective entity-wide security program.

**Response to the Report**

We issued the draft report to the Deputy Secretary on September 8, 2000. The Deputy Secretary provided a written response dated October 18, 2000 stating that the Office of the Chief Information Officer had reviewed the draft report and did not have any comments. The response did not indicate whether the Department agreed or disagreed with the findings and recommendations. It is included in Appendix C.

# TABLE OF CONTENTS

# Abbreviations

| | |
|---|---|
| CIAO | Chief Infrastructure Assurance Office |
| CICG | Critical Infrastructure Coordination Group |
| CIO | Chief Information Officer |
| CIPP | Critical Infrastructure Protection Plan |
| MEI | Mission Essential Infrastructure |
| NIPC | National Infrastructure Protection Center |
| OIT | Office of Information Technology |
| OMB | Office of Management and Budget |
| PDD | Presidential Decision Directive |

# Introduction

HUD processes over $31.5 billion worth of payment transactions and insures over $500 billion worth of both single and multifamily properties. In addition, many of HUD's data systems contain both privacy and sensitive financial data. A Departmental or entity-wide program for information security planning and management is necessary to protect the availability, integrity, and confidentiality of HUD's data and the systems they rely on.

The entity-wide information security program is the foundation of an entity's security control structure and a reflection of senior management's commitment to address security risks. An effective entity-wide security program should provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, monitoring computer-related controls, and training system users in computer security. Also, Presidential Decision Directive (PDD) 63, requires Federal agencies to protect their critical infrastructures, especially cyber-based systems, and to develop a plan for doing so. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. The General Accounting Office also designated information security as a government-wide high-risk area since 1997.

## Audit Objectives

The overall audit objective was to evaluate the adequacy of HUD's entity-wide security. Specifically, we determined whether HUD's entity-wide security program provided a framework and continuing cycle of activity for: (1) assessing and managing risk; (2) developing and implementing effective security policies and procedures; and (3) monitoring the effectiveness of those procedures. We also determined the adequacy of agency planning and assessment activities for protecting critical cyber-based infrastructure as required by PDD 63.

## Audit Scope and Methodology

We conducted the audit in accordance with generally accepted government auditing standards and performed our on-site work at HUD Headquarters. We interviewed key personnel within the Office of the CIO and the Office of Information Technology (OIT). For the audit, we obtained and reviewed applicable laws, regulations, policies, and handbooks. In addition we reviewed security-related and budget documentation to include risk assessments, application system security plans, system authorization statements, budget requests, and vulnerability assessment reports. We also reviewed the Department's Critical Infrastructure Protection Plan (CIPP) prepared in

accordance with the requirements of PDD 63. Our conclusions are based on analysis of the documentation obtained and the interviews conducted.

**Audit Period**

We performed our audit fieldwork from February 2000 through July 2000.

# HUD Has Not Adopted the Necessary Practices for Information Systems Security

The Clinger-Cohen Act requires the head of every executive agency to ensure that the information security policies, procedures, and practices of the executive agency are adequate. Despite the magnitude of HUD's systems in terms of dollars and transactions processed and prior reported security weaknesses, its security practices are still deficient. HUD has not adequately planned and managed an entity-wide security program to ensure that its critical information system resources are protected from accidental or intentional loss or damage. Specifically, the Department has not:

- assessed and managed risks on a continuous basis;
- documented and kept security plans current;
- monitored the security program's effectiveness, including establishing a security incident tracking, reporting, and response capability;
- provided mandatory training and awareness for all system users; and
- updated its Critical Infrastructure Protection Plan as required by PDD 63.

HUD has not adopted the above practices because the responsibility and accountability for information security are ill defined and fragmented. As a result, management support and funding for an information system security program have been limited, thereby placing HUD's critical information system infrastructure at risk.

## Risks Are Not Assessed and Managed on a Continuing Basis

Office of Management and Budget (OMB) Circular A-130 requires that agencies consider risk when determining the need for and selecting computer-related control techniques. It further states that security controls should be reviewed at least every three years. According to HUD Handbook 2400.24 REV-2, risk management involves an assessment of risk, the selection and implementation of cost effective controls, and periodic reviews of security controls.

HUD did not adequately assess and manage risks on a continuous basis as required. We examined OMB Circular A-130 compliance review reports for 22 HUD application systems. Under OIT's direction, a contractor conducted these reviews for the Department from FY 1997 to

FY 1999. Management accepted and used the reports to identify security risks, determine their magnitude, and identify areas needing safeguards. We found that for 19 of 22 (86%) application systems reviewed, risk assessments were not conducted on a regular basis. They are required at least every three years, or whenever systems, facilities or other conditions change. Without this required continuous effort, the Department cannot determine whether security measures are cost effective or updated to protect the confidentiality, integrity, and availability of HUD's data systems.

**Planned Internal Penetration Test Was Not Performed**

A risk management program should also include an assessment of network vulnerabilities. In today's modern computing environment, the network is the critical component of an information technology infrastructure. Penetration testing is an accepted practice used to determine vulnerabilities of a network as part of assessing risks. A network penetration test is defined as an activity whereby a team attempts to circumvent the security processes and controls of interconnected servers and workstations. Posing as either internal or external unauthorized intruders, the team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the network in what would be unauthorized ways.

During the FY 1998 and FY 1999 audit of agency financial statements, the OIG conducted a limited internal and external network penetration test and reported a number of vulnerabilities. Subsequent to the issuance of our reports, HUD hired a contractor to perform an external network penetration test with plans to also perform an internal test. However, management decided not to provide funding for the internal penetration test. Since there are thousands of internal users, contractor and Federal employees, it is critical that full penetration testing be performed to identify all of the network vulnerabilities.

# Security Plans Are Deficient

Another important aspect of entity-wide security is planning. OMB Circular A-130 requires agencies to plan for the adequate security of major applications, taking into account the security of all systems on which the applications will operate. Additionally, the Computer Security Act of 1987 requires Federal agencies to develop and implement

plans to safeguard systems that maintain sensitive data. The security plan describes the strategy for implementing information assurance and establishes a methodology for validating the security requirements identified in the security policy.

**Deficiencies in Security Plans Have Not Been Corrected**

The A-130 compliance reviews mentioned previously identified deficiencies in the application security plans that remain uncorrected. Although the reviews were performed from June 1997 through July 1999, security plans are still non-existent for four of the twenty-two application systems reviewed. Additionally, only one security plan was updated as recommended (F87-TRACS), whereas 8 were not updated at all and the remaining 9 reflected only partial updates as recommended. The results of our security plan analysis are summarized in Appendix A.

The review results showed that updates to security plans are needed in the areas of "system interconnectivity," "sensitivity or criticality ratings," and management "re-authorizations." System interconnectivity is important because all of HUD's critical systems send and receive data from other systems. The security plans for these systems must include steps to protect data integrity or data transmission from identified risks. Systems must also be rated in order to plan for the level of security efforts needed to minimize the risks of disclosure or alteration of data that would cause damage to the organizational or public interests. In addition, management "re-authorizations" should be done to indicate that the security plans are based on management acceptance of risk and security controls.

To be effective, security plans should be maintained to reflect current conditions. They should be periodically reviewed and, when appropriate, updated and reissued. This is done to reflect changes in risk resulting from factors such as changes in HUD's mission or types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all key personnel. Outdated plans not only reflect a lack of attention by top management, but also may not address current risks. Without updated security plans, HUD cannot implement the needed controls to minimize the security risks.

**Lack of Clearly Assigned Information Security Responsibilities and Accountabilities**

Another deficiency noted in the security plans is the lack of clear system ownership. OMB Circular A-130, Appendix III requires that the rules of the system and application "shall clearly delineate responsibilities and expected behavior of all individuals with access...and shall be clear about the consequences of behavior not consistent with the rules." The results of our review showed that most of the plans did not clearly identify who owned, used or relied on the various computer resources, especially data files, and ownership responsibilities. At best, some of the plans included "system rules of behavior" outlining responsibilities of systems users. However, the owners of the data files and application programs are generally managers of the program. The plans did not indicate the program manager primarily responsible for the proper operation of the program and for the accurate reporting of related computer data nor did they identify the system administrator. No formal document had been prepared that designates the responsible parties. Also, there was no indication as to whether a particular application system had multiple owners. Without clearly assigned ownership responsibilities, access authorizations may be left to personnel who are not in the best position to determine users' access needs. Such personnel are likely to authorize overly broad access in an attempt to ensure that all users can access the resources they need.

# Security Program Is Not Adequately Monitored

A security program should be monitored and periodically reassessed to ensure that policies continue to be appropriate and that the controls are accomplishing their intended purposes. The monitoring function should: (1) include management awareness and commitment to the security program, (2) follow through on recommended actions to correct reported deficiciencies, and (3) track, report and analyze security incidents. We found several weaknessess in security monitoring.

**No Management Authorization for 14 Critical systems**

OMB Circular A-130 requires that Federal agencies periodically review the security of their general support systems and major applications. It also requires that a management official authorize in writing the use of each general support system or major application based on

acceptance of risk and security controls. This is an important control to indicate that management has considered and accepted the risks as well as taken the appropriate actions for risk mitigation. We determined during our review that 14 out of 22 (64%) application systems examined lacked risk acceptance authorizations. Without this authorization, there is no assurance these critical systems are operating at an acceptable level of risk. Therefore, they could expose the Department to data compromise, loss or system damage.

**Lack of Follow-up on A-130 Reviews**

From FY 1997 to FY 1999, HUD spent approximately $470,000 for contractor-performed OMB A-130 compliance reviews. The purpose of these reviews is to determine compliance with appropriate security policies and procedures. Although these reviews identified numerous deficiencies, the Department did not effectively use the results to ensure security compliance. There is no process in place to follow up on recommended actions and to hold program managers accountable.

We examined the results of OMB A-130 compliance reviews to determine whether recommended corrective actions were implemented. HUD personnel informed us that the results of these reviews were forwarded to the respective Program Assistant Secretaries with a requirement for Program Managers to respond with a report detailing how recommendations would be implemented. However, many of the program offices did not respond and eventually this practice was discontinued. We found that Program Managers' responses were not submitted for 18 out of 22 (82%) risk assessments reviewed and follow-up monitoring was not performed to ensure the corrective actions were taken. According to OIT, an attempt was made to follow up on the requests for action plans to assure responses from program offices and hold them accountable for implementing recommendations. However, OIT encountered little success in its efforts to get program offices to cooperate. As a result, the investment in OMB A-130 compliance reviews has provided limited benefits for HUD's security program.

**Incident Response Capacity Needs Improvement**

OMB A-130 requires agencies to establish formal incident response mechanisms, make system users aware of these mechanisms, and educate users on how to use them. Security incidents, whether caused by viruses, hackers, or

software bugs, are becoming more common and can place valuable resources at risk. An effective security management program should provide the capability to identify, monitor and report security incidents. Data related to the incident should be collected and used to analyze the frequency and variety of security violations and any resulting damage. Security incident data can also provide valuable input for risk assessments, resource determination, and evaluation of control effectiveness.

Tracking and analyzing security incidents can provide a means of identifying emerging problems and assessing the effectiveness of current policies and awareness efforts. They can also help in determining the need for stepped up education of new controls to address problem areas and monitor the status of investigative and disciplinary actions. Finally, a formal tracking system will enable the Department to ensure that no individual violation is inadvertently overlooked and that violations are handled consistently.

**OIT Has Implemented Tool Intrusion Detection**

Due to the increased interconnection of computerized systems, an incident response mechanism should also facilitate the exchange of incident data with other Federal organizations. For many years, the Department did not have the means to detect and resolve incidents of intrusions into HUD's computer-based systems. Recently, OIT implemented RealSecure an automated, real-time intrusion detection and response system for computer networks. RealSecure provides around-the-clock network surveillance and automatic interception and response to security breaches and internal network abuses before systems are compromised. At the time of our review, the Department had developed a drafted set of procedures for implementing the intrusion detection tool and network monitoring. However, the Department has not implemented a formal process to report and resolve computer security incidents.

HUD has not implemented an automated information exchange capability. The Department did include a plan in the CIPP to establish a communication link with the National Infrastructure Protection Center's (NIPC) Watch and Warning Center for bi-directional information exchange. However, there is no evidence that funding is available or that an implementation schedule and milestones have been established. The link is essential to automatically

communicate all threat indications, warnings, and detailed information about hostile actions against HUD's cyber-based infrastructure to the NIPC. HUD should coordinate with the NIPC to expedite implementation of an automated information exchange process.

After a recent computer security incident, Federal Computer Week reported that a lack of coordination among the Federal organizations in charge of responding to cyber attacks led to a delayed delivery of warning and resulted in damage to system availability. The Government Accounting Office's review of the incident found that the NIPC, the Federal Computer Incident Response Capability, and the Defense Department's Joint Task Force for Computer Network Defense did not send out sufficient warnings and information about the incident until well after the damage occurred. HUD's Critical Systems Vulnerability Assessment dated March 2000, also noted that HUD's security plans did not address incident response procedures nor have formal incident response capability plans been prepared.

## Mandatory Security Training Has Not Been Provided to Users

The Computer Security Act of 1987 requires Federal agencies to provide mandatory periodic training in computer security awareness and accepted computer security practices. This includes all employees who are involved with the management, use, or operation of Federal computer systems within or under the supervision of that agency. OMB Circular A-130 requires training of individuals before granting access to systems or applications. The training is to make sure they are aware of system or application rules, their responsibilities, and their expected behavior.

HUD has not required that users obtain mandatory security awareness training before granting them access to HUD's systems. The current method of user training is to make security related materials available on the HUD Intranet, and periodically issue information security guide pamphlets and videotapes. While these security promotional techniques are attention getting and user friendly, they are noncompulsory.

A-130 reviews conducted by the Department also concluded that different levels of security training is consistently provided to system users. All 22 of the OMB A-130 compliance reports examined indicated that users did not receive periodic security training, either through the use of computer-based training or in a classroom setting. Also, 13 out of the 22 reports stated that specialized training was not consistently provided for users with different access levels, such as system and security administrators.

We expressed our concern that mandatory security training is not provided or required to OIT and CIO officials. They acknowledged this weakness and indicated that management does not consider security training a high priority. The Department has invested limited personnel and financial resources for security training.

Security training is a critical component of an information security program to ensure that users are knowledgeable of departmental security policies, practices, and risks. Without adequate security training, users may not be aware of the system or application rules and their responsibilities. This increases the risk of unintentionally disclosing sensitive information or causing damage to critical systems or data.

## Critical Infrastructure Protection Plan Needs Updating

Because of the substantial reliance on information technology and the increasing need to protect government information resources, the President issued PDD 63, requiring executive agencies, such as HUD, to prepare an entity-wide plan for protecting their critical infrastructures. This plan, known as Critical Infrastructure Protection Plan (CIPP), addresses the Department-wide information collection, processing, and management functions. The Critical Infrastructure Assurance Office (CIAO), an interagency office housed at the Commerce Department, is responsible for assisting agencies in developing their CIPP. A CIAO task force provided review comments on HUD's CIPP in March 1999. We examined HUD's updated plan to determine whether the agency took adequate action to implement the CIAO's recommendations. Although HUD

**Agency Mission Critical Infrastructure Assets Not Identified**

implemented many of the CIAO's recommendations, we found requirements that are still not addressed in the plan. The deficiencies identified by the CIAO, as well as the OIG's evaluation are summarized in Appendix B and described in detail below. The CIPP should identify essential agency missions and those critical infrastructure assets required to accomplish them. The CIAO's definition of agency internal assets includes physical facilities, computer facilities, and personnel. HUD has not updated its plan to include a detailed list of mission-critical personnel assets, or reference the availability of this detailed information, if the Department deems it confidential. The CIPP also lacks an outline of the overall process used for identifying external assets needed to support critical missions.

**Organizational Roles and Resoponsibilities Not Defined**

HUD's CIPP does not identify the organizational units and/or individuals responsible for critical infrastructure protection. It also does not describe the responsibilities of each unit and/or individual. Although HUD did include a description of the agency's organizational structure with regard to cyber-based and physical assets, there was no reference to the organization responsible for personnel assets and their respective role in carrying out critical infrastructure responsibilities.

**Resource Requirements Not Identified**

HUD's CIPP did not include a complete estimate of resources, both personnel and financial, required to achieve full compliance with PDD 63. An estimate of current and future resources is necessary to ensure the Department is able to protect its critical infrastructure from attacks. The CIAO recommended that the Department ensure that these needs be clearly justified and aggressively sought through supplemental and annual budget requests.

**Incomplete Identification of New Information Assets**

HUD's CIPP did not include an evaluation of new assets to determine whether they should be included in its Mission Essential Infrastructure (MEI). HUD had not considered personnel as an essential part of information resources. Specifically, it has not identified staff and management, including security management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services and information systems.

HUD also did not consider data as information resources. Specifically, it has not identified all data, both electronic and hard copy, and information required to support the

Department's mission. This includes numbers, characters, images or other methods of recording, in a form that can be assessed by a human or input into a computer.

HUD did not use the CIAO infrastructure asset evaluation survey to identify its MEI assets nor did the asset identification process include a determination of estimated replacement costs, planned life cycle, and potential impact to the Department if the asset is rendered unusable. Further, HUD did not establish milestones for identifying and reviewing its MEI. Therefore, HUD cannot provide feedback on whether it is meeting its milestones. Also, HUD's CIPP did not include a milestone for reviewing existing policies and procedures.

**No Security Planning for New Program with Critical Infrastructure Needs**

HUD's CIPP should require the Department to ensure that security planning procedures are incorporated into the basic design of new programs with critical infrastructure needs. It also did not require including provisions for: (1) risk management and assessments, (2) security plans for information technology systems, (3) command control and communications, (4) identification of classified or sensitive information, and (5) awareness and training measures. Further, the CIPP lacked a milestone for establishing procedures to ensure that the agency incorporates security planning into the basic design of new programs.

**Protection Measures Not Required as part of the Strategic Planning and Performance Measurement Process Required**

The CIPP should also require the Department to incorporate critical infrastructure protection measures in its strategic planning and performance measurement process. It also did not identify a milestone for incorporating the critical infrastructure protection functions into its strategic planning and performance measurement frameworks. Finally, although HUD has plans for continuous and periodic review of its threat environment, little progress has been made to meet initial implementation deadlines.

# CIO Role in Information Security Should Be Strengthened

HUD has neither placed sufficient priority nor devoted adequate resources to assure the necessary practices for information security are implemented. The establishment of the Office of the CIO, a senior level organization, almost two years ago provided an opportunity for the Department

to raise the priority and support for information security. However, the CIO has not fulfilled the management void in this critical area.

**CIO is in the Best Position to Provide Leadership, Oversight and Enforcement for Information Security**

Responsibility for information security is divided between three organizations. The CIO is responsible for security policy and oversight. OIT is responsible for administering system access and limited oversight through A-130 compliance reviews of specific applications. The program offices are responsible for protecting the data in the automated systems that support their business processes. These three groups, (CIO, OIT, and the program offices) are expected to work collaboratively to protect HUD's information systems.

The current approach to security lacks high level management support to ensure that the necessary practices for security are implemented. Since the CIO reports directly to the Secretary, it is in the best position to provide the necessary leadership, oversight, and enforcement for information security. However, the CIO's involvement in this area has been limited. In particular, the CIO has not specified its oversight responsibilities in the areas of risk management, security planning and monitoring, training and awareness, and the CIPP updates.

Another problem area related to oversight is the lack of enforcement. For instance, OIT has been responsible for A-130 compliance reviews but claims that it cannot require the program offices to address security deficiencies found in the reviews. OIT is viewed as a technical organization providing customer support to program offices rather than as an oversight organization with enforcement authority. In addition, OIT is two levels below most program offices. In order to gain cooperation from the program offices, compliance would have to be mandated from a higher level of authority such as the CIO. The CIO, because of its standing, has the sufficient authority to monitor compliance with policies, report results to senior management, and elevate concerns regarding inappropriate risk management decisions or practices.

**CIO should Control Funding Requests for Information Security**

Another concern is that under the current arrangement, both OIT and the CIO request funding for information security. Since the CIO is in a better position to raise the level of importance on information security, it should take the lead

for funding requests. This is clearly demonstrated for the FY 2000 budget. OIT requested $2.5 million for security and received only $300,000 while the CIO received most of the $1.136 million it requested. As a result of OIT's budget cuts, important initiatives such as security training and awareness, OMB A-130 compliance reviews, penetration testing, and security plans reviews were not funded.

## Deputy Secretary Comments

The Deputy Secretary provided a written response dated October 18, 2000 stating that the Office of the Chief Information Officer had reviewed the draft report and did not have any comments. The response did not indicate whether the Department agreed or disagreed with the finding and recommendations.

## OIG Comments

Although the Deputy Secretary's written response did not indicate whether they agreed or disagreed with the finding and recommendations, we did receive a verbal response from officials within the Office of the CIO indicating that they agreed with the finding and recommendations and fully intend to take corrective action.

## Recommendations

We recommend that the Deputy Secretary:

1. Assign the CIO full responsibility and accountability for information security and provide the adequate resources for its implementation.

2. Transfer information security responsibilities, with the exception of password and user ID administration, from the Office of Information Technology to the Office of the Chief Information Officer.

We recommend the Chief Information Officer complete the following actions after assuming full responsibility for information security:

3. Budget and plan for all information security related activities.

4. Develop an organizational charter to clarify security responsibilities.

5. Implement procedures to ensure that risks are assessed at least every three years, or whenever systems, facilities, or other conditions have changed.

6. Develop a plan for conducting OMB A-130 compliance reviews and implement follow up procedures to ensure that corrective actions are taken.

7. Coordinate with OIT to conduct an extensive independent penetration test for HUD's internal network.

8. Coordinate with OIT and program offices to ensure that appropriate security personnel develop, document and update security plans for all application systems.

9. Ensure that security plans include a clear identification of who owns, uses and relies on the various computer resources and their responsibilities as owners.

10. Ensure that management officials authorize in writing the use of each general support system and application systems.

11. Document and implement formal procedures for reporting and resolving detected intrusions.

12. Take steps to expedite implementation of the automated information exchange process, as outlined in the Critical Infrastructure Protection Plan, through coordination with the National Infrastructure Protection Center.

13. Ensure security plans address incident reporting procedures and establish formal Incident Response Capability Plans.

14. Institute mandatory security awareness for users prior to them being granted access to HUD systems.

15. Update the Critical Infrastructure Protection Plan to address the deficiencies in the report as summarized in Appendix B.

# Security Plan Analysis

| System Application | Date of Most Recent OMB A-130 Review | Most Recent Security Plan (1) | Updated Security Plan (2) | Implemented A-130 Review Recommendations (3) |
|---|---|---|---|---|
| A49 | Jun-97 | none | no | no (non existent) |
| A80S | Jun-97 | Nov-97 | yes | yes (partially) |
| A96 | Jun-97 | Nov-97 | yes | yes (partially) |
| F42 | Jun-97 | Dec-94 | no | no |
| F47 | Jun-97 | Aug-97 | yes | yes (partially) |
| F57 | Jun-97 | Aug-94 | no | no |
| F72 | Jun-97 | none | no | no (non existent) |
| F87 | Jun-97 | Jul-99 | yes | yes |
| A31 | Jun-98 | no date | ? | yes (partially) |
| A80R | Jun-98 | Oct-98 | yes | yes (partially) |
| A56 | Jun-98 | Mar-99 | yes | yes (partially) |
| A80D | Jun-98 | Oct-98 | yes | yes (partially) |
| F71 | Jun-98 | Feb-00 | yes | yes (partially) |
| F75 | Jun-98 | Oct-97 | no | no |
| G14 | Jun-98 | Oct-97 | no | no |
| PC-TARE | Jun-98 | none | no | no (non existent) |
| D21 | Jul-99 | Jan-98 | no | no |
| D64a | Jul-99 | Feb-00 | yes | yes (partially) |
| F17 | Jul-99 | Dec-94 | no | no |
| F90 | Jul-99 | none | no | no (non existent) |
| F46 | Jul-99 | Dec-94 | no | no |
| F49 | Jul-99 | Dec-94 | no | no |

LEGEND:

(1) "None" indicates that a security plan was not provided for our review. "No date" indicates that a security plan was provided; however, it was not dated.

(2) "No" indicates that the security plan provided was not updated since the OMB A-130 compliance review or one was not provided. "Yes" indicates that the security plan has been updated since the OMB A-130 compliance review. "?" indicates that we cannot determine whether the plan provided was an updated version.

(3) "No" indicates that a security plan has not been updated. "No (non existent)" indicates that a security plan did not exist. "Yes" indicates that a security plan was fully updated to reflect all of the A-130 compliance review recommendations. "Yes (partially)" indicates that security plans were partially updated to reflect some of the A-130 compliance review recommendations.

# Critical Infrastructure Protection Plan Deficiencies

| | Area of Concern | Deficiency Identified |
|---|---|---|
| 1. | Expert Review | a) HUD has not taken adequate remedial actions on deficiencies found during CICG expert review. |
| 2. | Organizational Roles and Responsibilities | a) CIPP does not adequately identify organizational units and/or individuals responsible for critical infrastructure protection, and describe the responsibilities of each unit and/or individual. |
| 3. | Resource Requirements | a) CIPP does not include a complete estimate of resources, both personnel and financial, required to achieve full compliance with PDD 63. |
| 4. | Identification of Information Assets | a) CIPP does not require an evaluation of new assets to determine whether they should be included in its MEI.<br>b) CIPP does not indicate whether HUD identified information resources to include people and data.<br>c) CIPP does not indicate whether HUD used the CIAO infrastructure asset evaluation survey to identify its MEI assets.<br>d) CIPP does not indicate whether the asset identification process includes a determination of its estimated replacement costs, planned life cycle, and potential impact on the agency if the asset is rendered unusable.<br>e) HUD has not established milestones for identifying and reviewing its MEI.<br>f) There is no indication of whether the agency is meeting its milestones. |
| 5. | Review of Existing Policies and Procedures | a) CIPP does not identify a milestone for reviewing existing policies and procedures. |
| 6. | New Program with Critical Infrastructures | a) CIPP does not require the agency to ensure that security planning procedures are being incorporated into the basic design of new programs that include critical infrastructures, including provisions for: (1) Risk management and assessments; (2) Security plans for information technology systems; (3) Security for command, control, and communications; (4) Identification of classified or sensitive information; and (5) Awareness and training measures to be taken for each program. |
| 7. | Strategic Planning and Performance Measurement | a) CIPP does not require the agency to incorporate its CIPP functions into its strategic planning and performance measurement frameworks.<br>b) CIPP does not identify a milestone for incorporating its critical infrastructure protection functions into its strategic planning and performance measurement frameworks. |
| 8. | Continuous and Periodic Review | a) CIPP does not indicate whether HUD plans for the continuous/periodic review of its threat environment appear adequate, and whether the agency is complying with these plans. |

# Deputy Secretary Comments

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
THE DEPUTY SECRETARY
WASHINGTON, D.C. 20410-0050

October 18, 2000

MEMORANDUM FOR: Kathryn M. Kuhl-Inclan, Assistant Inspector General, Office of Audit, GA

FROM: Saul N. Ramirez, Jr., Deputy Secretary, SD

SUBJECT: Draft Audit Report on HUD's Entity-wide Security Program

This is in response to Benjamin Hsiao's memorandum of September 8, 2000, regarding the Office of the Inspector (OIG) General Draft Audit Report on HUD's Entity-wide Security Program. The Office of the Chief Information Officer has reviewed the draft report and does not have any comments.

If you have any questions, please contact Pam Woodside, Director, Office of Systems Integration and Efficiency or R. John Haines, Critical Infrastructure Assurance Officer, in the Office of the Chief Information Officer, on 708-2050.

# Distribution

Chief of Staff, S, (Room 10000)
Acting Assistant Secretary for Congressional & Intergovernmental Relations, J (Room 10120)
General Deputy Assistant Secretary for Administration, A (Room 10110)
Deputy Assistant Secretary for Public Affairs, W (Room 10222)
Deputy Assistant Secretary for Administrative Services, Office of Executive Secretariat, AX (Room 10139)
Acting Deputy Chief of Staff, S (Room 10226)
Deputy Chief of Staff for Program and Policy, S (Room 10226)
Special Counsel to the Secretary, S (Room 10226)
Executive Officer for Administrative Operations and Management, S (Room 10220)
General Counsel, C (Room 10214)
Assistant Secretary for Housing-Federal Housing Commissioner, H (Room 9100)
Assistant Secretary for Policy Development and Research, R (Room 8100)
Assistant Secretary for Community Planning and Development, C (Room 7100)
Assistant Deputy Secretary for Field Policy and Management, SDF (Room 7108)
Assistant Secretary for Fair Housing and Equal Opportunity, E (Room 5100)
Director, Office of Departmental Equal Employment Opportunity, U (Room 5128)
Assistant Secretary for Public and Indian Housing, P (Room 4100)
Chief Information Officer, Q (Room P8204)
Chief Procurement Officer, N (Room 5184)
Director, Office of Information Technology, AMI (Room 4160)
Chief Financial Officer, F (Room 2202)
Director, Office of Departmental Operations and Coordination, I (Room 2124)
Acting Director, Enforcement Center, V (Portal Building)
Director, Real Estate Assessment Center, X (Portal Building)
Audit Liaison Officer, A (Room 10110)
Audit Liaison Officer, CFO (Room 2206)
Acquisitions Librarian, Library, AS (Room 8141)
Inspector General, G (Room 8256)
Deputy Inspector General, G (8256)
Counsel to the IG, GS (Room 8260)
Public Affairs Officer, G (Room 8256)
Assistant Inspector General for Audit, GA (8286)
Deputy Assistant Inspector General for Audit, GA (8286)
Director, Housing and Community Development Issue Area, U.S. GAO, 441 G Street, NW., Room 2474, Washington, DC 20548; ATTN: Judy England-Joseph
Director, Office of Federal Housing Enterprise Oversight, 1700 G Street, NW., Room 4011, Washington, DC 20552; ATTN: Armando Falcon
Ms. Cindy Fogleman, Subcommittee on Oversight and Investigations, Room 212, O'Neil House Office Bldg., Washington, DC 20515
Mr. Stanley Czerwinski, Associate Director, Resources, Community, and Economic Development Division, General Accounting Office, 441 G Street, Room 2T23, Washington, DC 20548
Mr. Steve Redburn, Chief Housing Branch, Office of Management and Budget, 725 17th Street, NW.,Room 9226, New Executive Office Building, Washington, DC 20503

The Honorable Fred Thompson, Chairman, Committee on Governmental Affairs,
340 Dirksen Senate Office Building, United States Senate, Washington, DC 20510
The Honorable Joseph Liberman, Ranking Member, Committee on Government Affairs,
706 Hart Senate Office Building, United States Senate, Washington, DC 20510
The Honorable Dan Burton, Chairman, Committee on Government Reform,
2185 Rayburn Building, House of Representatives, Washington, DC 20515
The Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform,
2204 Rayburn Building, House of Representatives, Washington, DC 20515