OFFICE OF THE INSPECTOR GENERAL

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-4500

Audit-Related Memorandum
No.01-DP-0802

September 6, 2001

MEMORANDUM FOR: Gloria Parker, Chief Information Officer, Q

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

SUBJECT: Annual Evaluation of HUD's Security Program and Practices

In accordance with the requirements of the Government Information Security Reform Act (GISRA), this audit memorandum presents the results of our annual evaluation of HUD's security program and practices. The objective of our evaluation was to determine whether the Department's security program is effective. During our evaluation, we performed procedures designed to ascertain whether the Office of the Chief Information Officer (OCIO) has: (1) developed and implemented effective security policies and procedures; (2) monitored the effectiveness of those procedures; and (3) coordinated the timely and effective implementation of actions to correct known security weaknesses. We also performed procedures to determine whether the Department has met the requirements of the Act by: (1) incorporating information security throughout the system lifecycle; (2) establishing an incident response capability to detect, report, and respond to security incidents; and (3) evaluating the effectiveness of its information security program.

Authority and Scope:

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform Act (GISRA)." The Security Act codifies the existing requirements of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" and requires agencies to incorporate security into the lifecycle of information systems. The Act also requires agency security program reviews, Inspector General security evaluations, and a report to OMB for inclusion in a government-wide report to Congress, annually.

We conducted this evaluation in accordance with generally accepted government auditing standards and performed our fieldwork at HUD Headquarters. We interviewed key personnel in

OCIO and the Office of Information Technology (OIT). As part of our evaluation, we reviewed applicable laws, regulations, policies, and handbooks. In addition, we obtained and reviewed security and budget related documentation to include draft security program plans and policies, application system security plans, system authorization statements, budget reports, and self-assessment reports. We also completed a survey of previously issued OIG audit reports to identify security weaknesses reported over the past three years that remain uncorrected. Long before enactment of the Act, our office routinely evaluated and reported on HUD's information security practices and the adequacy of security controls. Our audits included tests and procedures on a subset of HUD's general support systems and major applications to determine the effectiveness of information security controls.

Background:

HUD information systems process or track disbursements of over $31.5 billion and are used to account for insurance liabilities in excess of $500 billion for both single and multifamily property mortgages. The Department provides funding to a broad range of grant recipients throughout the country, as well as rent and operation subsidies. These subsidies benefit over 7 million lower income households through a variety of programs, including Public Housing and Section 8. HUD's systems also contain privacy and sensitive personal data needing protection from intentional or accidental disclosure or damage. Despite the magnitude of potential loss and the sensitive nature of HUD data, the Department's entity-wide security program is inadequate and cannot be relied on to ensure critical information system resources are protected from accidental or intentional loss or damage.

HUD has a long history of weak security practices. In 1994, GAO reported that the Department did not provide proper security over sensitive computer systems and data. Specifically, GAO reported that HUD had not:

- identified all of its computer systems that process sensitive or privacy data or prepared up-to-date and accurate security plans for these systems;
- established effective controls to prevent unauthorized individuals from accessing data contained in the Department's most sensitive computer systems;
- ensured that required background investigations have been completed on the hundreds of HUD and contractor personnel who operate, manage, maintain, or use the computer systems; or
- performed adequate computer security monitoring and training to ensure that sensitive computer data are properly controlled and safeguarded.

On October 31, 2000, the OIG issued an audit report on "HUD Entity-wide Security Program." Despite the six-year time lapse between the two reviews, we found that many of the security weaknesses reported by GAO remained uncorrected. Specifically, HUD still did not: (1) update or complete critical system security plans in a timely manner; (2) monitor its security program; and (3)

institute a mandatory security training program. We also found that risks are not assessed and managed on a continuing basis. Our report included several recommendations to the Deputy Secretary and the CIO aimed at strengthening the Department's security program and correcting security control weaknesses.

Our Concerns:

Subsequent to the issuance of our October 2000 report, the Secretary transferred responsibility and accountability for information security from the Office of Administration to the OCIO. The OCIO has a draft plan for establishing and maintaining an effective, comprehensive IT security program at HUD, "Information Technology Security Program Plan" dated December 2000. There are seven components outlined in the OCIO's security plan: (1) formulate security policies, standards, procedures and metrics; (2) assess risks; (3) design an IT security road-map based on the results of the risk assessment; (4) select and implement solutions; (5) conduct cost effective training; (6) monitor security; and (7) implement incident response and recovery.

We made inquiries to determine what progress the OCIO has made toward implementing its Plan. We observed some improvement in the following areas: draft security policies and plans have been documented; a preliminary security training program has been established; senior security managers were designated for each program area; and an incident response and recovery plan has been formalized. During FY 2001, the OCIO initiated the planning and program development for an entity-wide security awareness and training program. The program provides for an awareness briefing for HUD employees; however, to date only 584 of HUD's employees and contractors have completed the training. At the time of our review, OCIO officials were investigating computer-based security training solutions and finalizing an approach to ensure all HUD employees receive training on a continual basis.

On August 14, 2001, the OCIO requested that HUD program areas designate a representative to serve as Senior Security Manager. Each program area security manager will work with the security team and the Critical Infrastructure Assurance Officer (CIAO) to plan, coordinate, budget, manage, and implement HUD's Enterprise Information Systems Security Program.

Despite the improvements noted above, the Department still has not placed adequate emphasis on information security. The information security program lacks executive level leadership and direction, and previously reported weaknesses in management, operational, and technical controls remain uncorrected. Security monitoring activities were limited to the OCIO performance of its program evaluation as required by the Act. The evaluation was delayed and thus not likely to produce reliable results.

To meet the requirements of the Act, the OCIO requested that each program area complete the NIST "Self-Assessment Guide for Information Technology Systems." However, the request went out July 24, 2001 with a deadline for completion of August 27, 2001. The short turn around time for completion of the assessments and delivery of the results is inadequate. Program officials expressed confusion as to how to use the assessment guide and requested guidance from our office. To improve

the usefulness and reliability of the results of program area self-assessments, the OCIO must provide adequate guidance and direction on how to complete the assessments. In addition, the OCIO security staff should establish a process and allow time to review the results for completeness and accuracy and to provide proper oversight.

Executive level leadership and direction is required to ensure successful implementation of HUD's agency-wide security program. HUD's CIAO is responsible for the overall infrastructure protection and execution of the Information System Security Program. The CIAO establishes Departmental information systems security policies, procedures, standards and guidelines and provides oversight to ensure the effective implementation of security controls. However, the CIAO is a staff level position reporting to the Director of the CIO's Office of Systems Integration and Efficiency, two levels beneath the CIO. If the CIAO reported directly to the CIO, it would strengthen their ability to communicate program goals and objectives, solicit support in meeting resource requirements, and increase their authority to coordinate activities with senior level program officials. In FY 2001, implementation of the OCIO's entity-wide security program plan was hampered further when the CIAO position was vacated more than six months ago without a replacement.

To determine the status of previously reported security weaknesses, we surveyed audit reports issued during the period October 1, 1999 through March 31, 2001. Including the October 2000 report on Entity-wide security, we issued 11 audit reports that identified security control weaknesses. Eight audit reports remain open because final corrective actions are not yet complete; 28 recommendations with OIG approved management decisions on proposed corrective actions (final action on 3 of the 28 are late) and 2 recommendations to which we disagree on the Department's proposed corrective action and no final agreement for resolution has been reached.

Significant security control weaknesses identified in these audit reports are listed below, in accordance with categories used in the NIST Self Assessment Guide – management, operational, and technical controls. Management controls focus on the management of the IT security system and the management of risk for a system. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Specific management weaknesses identified during previous audits and for which audit recommendations remain open follow:

- a risk management program that includes risk assessment, risk mitigation, and risk maintenance has not been established and security is not managed and planned for throughout the IT system lifecycle;

- security controls are not routinely evaluated by the OCIO and corrective actions noted by independent reviewers are not implemented in a timely manner (outstanding audit issues and corrective actions recommended in prior OMB A-130 reviews);

- risk assessments are not performed and document on a regular basis and related management approvals (certification and accreditation) have not been documented;

- system security plans are not updated and completed in a timely manner; and
- periodic reviews are not performed to ensure adequate privacy on HUD's Internet web pages, including those web pages maintained at and by external contractors.

Operational controls address security methods focusing on mechanisms primarily implemented and executed by people, as opposed to systems. These controls are designed to improve the security of a particular system or group of systems. Specific operational weaknesses identified during previous audits and for which audit recommendations remain open include:

- controls over mainframe systems are not adequate to provide assurance that computer resources (mainframe data and application data) are protected from unauthorized modification, disclosure, loss, or impairment, and are operated in accordance with established federal security requirements;

- inadequate separation of duties at grantee organizations utilizing CPD's Integrated Disbursement Information System;

- personnel security over critical and sensitive systems' access has been inadequate - a process needs to be developed to ensure that only authorized individuals with the appropriate position sensitivity level of clearance is granted access to HUD critical systems;

- application controls over Housing's systems do not ensure that data relied upon by management is complete and accurate;

- the OCIO has not included the OIG as an integral part of the Department's security incident reporting process; and

- internet privacy statement does not contain an appropriate disclaimer regarding the security of privacy data transmitted via the Internet and web pages and contracted Internet web sites do not include a hyperlink to Department's standardized privacy statement.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Specific technical control weaknesses identified during previous audits and for which audit recommendations remain open include:

- inadequate protection over sensitive programs and files on the Unisys mainframe – program and files containing sensitive information about customers and sensitive system activities are accessible using low level user accounts;

- no audit trail mechanism to trace individual use of the HUDSEC privilege, the most powerful authorization used for performing Unisys security and system administration functions;

- HUD's Central Accounting and Program System's system administrators are allowed access to data and privileges in excess of those required to accomplish their job function;

- network security controls need improvement - servers set to allow unencrypted password logins, network operating system files (the bindery) were not protected from unauthorized access and a significant number of users with easily guessed passwords;

- field information technology offices do not conduct periodic tests of backup tapes as recommended; and

- critical applications are still not fully implemented under configuration management.

Conclusion:

In conclusion, we found that the security-monitoring program still needs strengthening, the information security program lacks executive level leadership and direction, and previously reported weaknesses in management, operational, and technical controls remain uncorrected. As a result, the absence of an effective entity-wide security program, proactive leadership from the Office of the CIO, and adequate management, operational, and technical controls, may lead to insufficient protection of sensitive or critical resources and compromise the integrity, confidentiality, reliability, and availability of information maintained in HUD's systems.

Recommendations:

We recommend that the Chief Information Officer:

1. Provide adequate resources and authority to the Critical Infrastructure Assurance Officer to enable successful implementation of the Entity-wide Security Program Plan as outlined.

2. Provide guidance, direction, and oversight to program area Senior Security Managers on the performance of security assessments and establish procedures to review the results for completeness and accuracy that include specific tests designed to evaluate the effectiveness of security controls.

3. Proactively monitor and oversee the Departments security program and ensure that security weaknesses noted during independent and internal reviews of program specific systems are effectively corrected.

Distribution

Secretary, S
Deputy Secretary, SD
Chief of Staff, S
Acting Associate General Deputy Assistant Secretary for Administration, A
Deputy Chief of Staff for Policy & Programs, S
Deputy Chief of Staff for Intergovernmental Affairs, J
Senior Advisor to the Deputy Secretary, S
Executive Officer for Administrative Operations and Management, A
General Counsel, C
Assistant Secretary for Housing/Federal Housing Commissioner, H
Acting Assistant Secretary for Policy Development and Research,
Assistant Secretary for Community Planning and Development, C
Acting Assistant Secretary for Fair Housing and Equal Opportunity, O
Acting Assistant Secretary for Public and Indian Housing, P
Chief Financial Officer, F
Acting Director, Enforcement Center, V
Acting Director, Real Estate Assessment Center, X
Acting Inspector General, GA
Assistant Inspector General for Audit, GA
Deputy Assistant Inspector General for Audit, GA
Acquisitions Librarian, Library, AS
Audit Liaison Officer, A
Audit Liaison Officer, F
Sharon Pinkerton Senior Advisor, Subcommittee on Criminal Justice,
Drug Policy & Human Resources, B373
Rayburn House Office Bldg., Washington, DC 20515
Cindy Fogleman, Subcommittee on Oversight and Investigations
O'Neil House Office Bldg., Room 212
Washington, DC 2051
Stanley Czerwinski, Associate Director, Housing and Telecommunications Issues
United States General Accounting Office
441 G Street, NW., Room 2T23
Washington, DC 20548
Steve Redburn, Chief Housing Branch, Office of Management and Budget,
725 17th Street, NW, Room 9226,
New Executive Office Bldg.
Washington, DC 20503

The Honorable Fred Thompson, Ranking Member,
Committee on Governmental Affairs, 340 Dirksen
Senate Office Bldg., United States Senate,
Washington, DC 20510
The Honorable Joseph Lieberman, Chairman,
Committee on Government Affairs, 706 Hart Senate
Office Bldg., United States Senate
Washington, DC 20510
The Honorable Dan Burton, Chairman, Committee on Government Reform,
2185 Rayburn Bldg.,
House of Representatives
Washington, DC 20515
The Honorable Henry A. Waxman, Ranking
Member, Committee on Government Reform
2204 Rayburn Bldg., House of Representatives,
Washington, DC 20515
Andy Cochran, House Committee on Financial Services
2129 Rayburn H.O.B
Washington, DC 20515