Issue Date: October 30, 2002
Audit Case Number: 2003-DP-0801

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

//Signed//

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

SUBJECT: AUDIT MEMORANDUM -Annual Evaluation of HUD's Information Security Program

INTRODUCTION

We completed an audit of the Department of Housing and Urban Development's (HUD's) information security program and practices as required by the FY 2001 Defense Authorization Act (P.L. 106-398) Title X, subtitle G, "Government Information Security Reform (GISRA)." The Act requires that the Office of Inspector General (OIG) perform an annual independent evaluation of the Department's information system (IS) security program leading to a conclusion regarding its overall effectiveness. The purpose of the Act is to provide a comprehensive framework for establishing and ensuring the effectiveness of information system security programs, including the management, oversight, and controls over information resources that support Federal operations and assets.

We performed our audit at HUD Headquarters within the Office of the Chief Information Officer (OCIO) between May 2002 and August 2002. To meet our objectives, we: (1) determined progress made toward correcting deficiencies reported in the Department's Plan of Action and Milestone (POA&M) and OIG audit reports; (2) evaluated the OCIO's information security evaluation and remediation approach; and (3) ascertained progress made toward implementation of HUD's Critical Infrastructure Protection Plan (CIPP). We performed our audit in accordance with Generally Accepted Government Auditing Standards.

In accordance with HUD Handbook 2000.06 REV-3, within 60 days please provide us, for each recommendation without a management decision, a status report on: (1) the corrective action taken; (2) the proposed corrective action and the date to be completed; or (3) why action is considered unnecessary. Additional status reports are required at 90 days and 120 days after report issuance for any recommendation without a management decision. Also, please furnish

us copies of any correspondence or directives issued because of the audit. Should you or your staff have any questions, please contact me at 202-708-0614, extension 8149.

SUMMARY

Subsequent to issuance of our report, "Annual Evaluation of HUD's Security Program and Practices" (2001-DP-0802), dated September 6, 2001, the OCIO renewed its commitment to take corrective actions and implement program enhancements intended to eliminate longstanding weaknesses and to strengthen its entity-wide IS security program. Our evaluation of HUD's entity-wide IS security program focused on determining what progress has been made to complete these initiatives as well as the OCIO's information security evaluation and remediation approach. In addition, we made inquires to determine the progress made toward implementation of HUD's CIPP.

While we observed improvement in some aspects of HUD's IS security program, weaknesses persist. Delays in the implementation of corrective actions and tasks designed to strengthen its IS security program continue to put critical data and resources at risk. Although the OCIO expanded its self-assessment program in FY 02, we found that the results reported are unreliable in the absence of a review process to ensure correct performance of the assessments. We also found that despite the effort given to prepare its CIPP, the OCIO has made little progress in implementing tasks outlined in the plan to strengthen its IS security program in the areas of risk management, emergency management and interagency coordination, recruitment, education, and awareness.

We attribute these delays to funding limitations, poor planning and coordination, and administrative processes preventing the timely establishment of contractual agreements. As a result, progress toward strengthening HUD's entity-wide IS security program has been hampered and the program remains immature thereby, not fully effective in ensuring the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting Departmental operations and assets.

The OCIO should strengthen its IS security program to ensure prompt correction of weaknesses noted during independent and internal reviews of its information systems. In addition, the OCIO should expand the self-assessment program to include the review and verification of a sample of the self-assessments completed by program officials. In order to accomplish the objectives of the CIPP, the OCIO must promptly allocate adequate resources and mandate timely completion of initiatives outlined in the plan.

BACKGROUND

HUD's 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. HUD provides funding to a broad range of grant recipients throughout the country, as well as rent and operating subsidies. These subsidies benefit over 7 million lower income households through a variety of programs, including Public Housing and Section 8. The

Department also insures over $500 billion worth of single and multi-family properties. In addition, many of HUD's data systems contain personal privacy and sensitive financial data. HUD's interoperable IS infrastructure increases risk by allowing access to an increased number of external individuals and organizations, resulting in increased opportunity for exploitation of its vulnerabilities. The OCIO's should make it a priority to mitigate the risk of intentional or accidental disclosure or damage to HUD data and information system resources.

Protecting the information and information systems on which the Federal government depends, requires the identification and resolution of known security weaknesses and risks, as well as a program to monitor and address future vulnerabilities and threats. Fulfilling the requirements of the GISRA is the first step toward meeting this priority. The OCIO's primary responsibilities under the GISRA are to:

- Ensure the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets;

- Develop and implement information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and

- Ensure that the agency's information security plan is practiced throughout the life cycle of each agency system.

FINDING 1

HUD Data and Information System Resources are at Risk of Intentional or Accidental Disclosure or Damage Due to Weaknesses in the Information System Security Program

During our audit, we found that delayed implementation of planned corrective actions and program enhancements, weak controls over the OCIO's security assessment program and failure to implement initiatives outlined in its critical infrastructure protection plans continue to put HUD data and critical information system resources at risk of intentional or accidental disclosure or damage. We determined that funding limitations, poor planning and coordination, and failure to establish contractual agreements in a timely manner has hampered progress toward strengthening HUD's entity-wide information system security program. As a result, the program remains immature thus, not fully effective in ensuring the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets. OMB Circular A-130 requires federal agencies to "implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Each agency's program shall implement policies, standards, and procedures which are consistent with government-wide policies, standards, and procedures."

Longstanding Information System Security Control Weaknesses Persist

To determine progress made to correct reported information security weaknesses, we obtained and reviewed the OCIO's Plan of Action and Milestones (POA&M) prepared in October 2001, quarterly updates to OMB, and IG reports completed since issuance of our FY 2001 GISRA evaluation report. We determined that the following reported significant security control weaknesses remain uncorrected. We categorized these weaknesses in accordance with the categories used in the National Institute of Standards and Technology (NIST) Self Assessment Guide (Special Publication 800-26) – 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. Operational controls address security methods focusing on mechanisms primarily implemented and executed by people, as opposed to systems. 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. Weaknesses identified during previous audits and for which audit recommendations remain open include:

Management Controls:

- 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;

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

- System security plans are not updated and completed in a timely manner; the OCIO has not updated security plan policies and procedures or prepared security plans for mission critical systems in compliance with OMB Circular A-130 or NIST Publication 800-18 guidelines.

Operational Controls:

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

- Personnel security over critical and sensitive systems' access is inadequate – the process to ensure only authorized individuals with the appropriate clearance are granted access to HUD critical systems needs to be improved;

- Application controls over HUD systems do not ensure that data relied upon by management is complete and accurate; and

- The OCIO has not included the OIG as an integral part of its security incident reporting process. Although, the Computer Incident Response Program document dated September 2001 states that "depending on the nature of the incident, additional investigations may be conducted by the HUD Internal Audit Office or the Office of the Inspector General," a reporting process has not been formalized.

Technical Controls:

- Controls over sensitive programs and files on the Unisys mainframe are inadequate;

- System administrators are allowed access to data and privileges in excess of those required to accomplish their job function;

- Network security controls need improvement - there are a number of vulnerabilities in the configuration and control of network resources;

- Field offices continue to operate with inadequate security controls over critical resources; and

- Critical applications are still not fully under configuration management control.

OCIO's Security Self-Assessment Program Does Not Include a Timely Review of Results

During fiscal year 2001, the OCIO required program officials to participate in the completion of the NIST Security Self-assessments in accordance with the guidance provided in NIST Special Publication 800-26. In fiscal year 2002, the OCIO expanded this review program to include all information systems in HUD's inventory. We commend the expanded self-assessment process; however, we found that the OCIO has not instituted a review process to ensure the completeness and accuracy of the completed assessments. The results of these reviews have limited value in the absence of a process to ensure the responses are reasonable. Additionally, the OCIO's involvement in the assessment process is limited to contractor oversight. We believe that a process to verify a sample of the results of the self-assessments would strengthen the OCIO's information security assessment program. In addition, active participation by OCIO officials would ensure proper correlation and presentation of assessment results to accurately portray the status of the Department's information system security program.

Although the NIST Self-Assessment Guidance Special Publication (800-26) recommends that the individuals assessing the system (the owners of the system or persons responsible for operating or administering the system) conduct the analysis of completed questionnaires, HUD has delegated this responsibility to a contractor. Contract personnel with little knowledge and understanding of HUD systems and operations evaluated and extrapolated the results summarized in the executive summary. Additionally, the results of the self-assessments are used to develop HUD's updated POA&M due to OMB on October 1, 2002.

OCIO officials forwarded copies of the completed self-assessments as they came in from the program areas. Although the OCIO deadline for completion was the week of July 22 – 26, 2002, they continued to come in as late as August 16, 2002. We received 143 files containing self-assessment questionnaires. Due to timing, resources, and the OCIO's inability to provide us with an extract of the contractor's database used to record and tabulate the self-assessment results, we were unable to perform a complete analysis of the responses. However, we did perform a cursory review of five of the complete questionnaires, including one for HUD's General Support System. After examining the questionnaires, we discussed with OCIO officials our concern regarding the reliability of the self-assessments. For example, our examination of the General Support System self-assessment, found that program officials indicated a level five for all critical elements, and associated sub-elements. According to NIST guidance, attaining level five means the organization has established, implemented, and fully integrated, within program operations, and procedures, controls to address the specified objective. In light of persistent weaknesses reported in HUD's general and application controls, including recently reported weakness in its networked environment, we are positive that the Department has not attained a level five in all critical elements for its General Support System (HUD's data processing infrastructure – mainframes, networks, etc.). We also examined four other completed self-assessments provided by the OCIO and found they did not include supporting documentation or written clarification of mitigating factors taken into consideration while completing the assessment form per NIST guidance. If not completed properly, results derived from the self-assessments will affect the accuracy and reliability of performance measures presented and may lead to erroneous conclusions.

Despite our concerns, the OCIO proceeded to formulate performance measures for its FY 02 GISRA report to OMB without validating the self-assessment responses. The OCIO derived the results presented by assigning a level of compliance for each critical element on the NIST questionnaire to a Federal Information System Controls Audit Manual (FISCAM) control category. Within each category, they tabulated the number of weaknesses reported for all the analyzed systems. The OCIO then calculated a non-compliance or weakness percentage by dividing the number of actual weaknesses by the maximum number of possible weaknesses in each category. By subtracting the non-compliance or weakness percentage from 100, a compliance percentage was calculated.

According to the NIST Self-Assessment Guide, "to project an accurate picture, the results must be summarized by system type, not totaled into an overall agency grade level." However, the OCIO has combined the results of all of the system self-assessments performed and represented them as a department-wide degree of compliance by FISCAM category. As indicated in the NIST guidance, it is inappropriate to combine the results of the one self-assessment of HUD's General Support System with the results of approximately 123 major applications, which operate on HUD's data processing infrastructure. Combined, you cannot derive a level of compliance that is meaningful or representative of the state of HUD's information security program nor get a true picture of progress made to strengthen the security program overall.

OCIO's CIPP is not Fully Implemented

In response to Presidential Decision Directive 63, the OCIO developed a Critical Infrastructure Protection Plan (CIPP), dated June 30, 1999. The CIPP outlines the OCIO's approach to

minimize vulnerabilities in HUD's information technology infrastructure that may influence achievement of critical missions. The plan outlines strategies, with short and long-range goals, to ensure the establishment of a successful critical infrastructure support program. The CIPP includes several initiatives designed to strengthen information system security in the areas of risk management, emergency management and interagency coordination, recruitment, education, and awareness. However, we found that little to no progress has been made toward implementation and completion of tasks identified in the CIPP.

Risk Mitigation

HUD has not fully implemented its Critical Infrastructure Protection Plan (CIPP) requirements for risk mitigation. Specifically, HUD has not: (1) completed planned risk assessments of the three Administrative Service Centers (ASC); (2) implemented risk mitigating countermeasures identified during vulnerability assessment of its three main computer processing centers; (3) conducted security reviews (in accordance with OMB Circular A-130) for its application systems; (4) updated security plan policies and procedures nor prepared security plans for mission critical systems in compliance with OMB Circular A-130 or NIST Publication 800-18 guidelines.

According to the CIPP, the OCIO planned to conduct risk assessments at HUD's three main computing centers and the three ASC offices between the period of September 1999 and January 2000. The ASC offices are located in New York City, Atlanta, and Denver. Organizations located at the ASC offices provide administrative resource services, and IT services for all of HUD's program field office locations and staff located in the field. Risk assessments include reviews of the physical facility security posture, network architecture, information security procedures and policies, resource utilization and requirements, policies and daily operational procedures, and threat profiles highlighting likely threats based on identified vulnerabilities as well as, where applicable, the performance of network penetration testing. During FY 2001 and FY 2002, the OCIO completed a vulnerability assessment of its three main computing centers and penetration testing on its Wide-Area Network. However, during our evaluation OCIO officials informed us that risk assessments of the ASCs were not completed, and are no longer planned.

Additionally, we found that the OCIO has not taken steps to address the vulnerabilities identified in the July 31, 2000 vulnerability assessment report of the HUD Headquarters Facilities (which included HUD Headquarters, HCC, and the DRF). Although the CIPP did not provide a timeline for implementing countermeasures to address vulnerabilities identified, we believe that prompt action to correct weaknesses is a key step in risk mitigation. The assessment identified several vulnerabilities, which if left uncorrected, could adversely affect HUD's critical infrastructure. OCIO officials stated they did not implement countermeasures outlined in the vulnerability assessment because management did not think that implementing countermeasures was necessary since they were in the process of negotiating a replacement IT outsourcing contract. OCIO officials did not provide documentation evidencing the performance of a cost benefit analysis and management instructions to forgo these corrective actions.

According to the NIST "Generally Accepted Principles and Practices for Securing IT Systems" (September 1996), risk mitigation involves the selection and implementation of security controls

to reduce risk to a level acceptable to management. OMB Circular A-130 requires that agencies consider risk when determining the need for and selecting computer-related control techniques. It further states that an agency should review security controls at least every three years. Further, HUD Handbook 2400.24 REV-2 specifies that risk management involve an assessment of risk, the selection and implementation of cost effective controls, and periodic reviews of security controls.

Emergency Management and Interagency Coordination

Despite ongoing initiatives to improve its Information Technology Security program, the OCIO still has not fully implemented its emergency management program. According to HUD's CIPP, the goal of its emergency management program is to formulate a critical infrastructure protection plan designed to establish and coordinate the exchange of information within and to and from HUD pertaining to critical infrastructure threats and warnings, as well as response and reconstitution actions in the event of damage to HUD's critical infrastructures. The CIPP calls for the full and rapid exchange of indication and warning information pertaining to threats to HUD personnel, information, and property. At the time of its development, the CIPP indicates that the OCIO was reviewing the best means of establishing a permanent bi-directional connectivity between the National Infrastructure Protection Center's (NIPC) Watch and Warning Center and OCIO officials. Further, the OCIO was to evaluate and select electronic connectivity solutions to meet this need.

Although the OCIO has documented a Computer Incident Response Program (CIRP), dated September 2001, the OCIO still has not fully implemented an incident-reporting mechanism (allowing HUD employees or contractors to report threat indications and warnings or direct actions against the Department's critical infrastructure). In addition, the OCIO did not provide evidence of establishing a communications link with the NIPC Watch and Warning Center to facilitate bi-directional information exchange. As of July 31, 2002, the OCIO reports that it is still in the process of initiating implementation of a nationwide incident response and handling program to establish policy to deter, detect, protect, respond and report both national and local cyber threats to the CIO and Chief Technology Officer in a timely manner for appropriate action. Additionally, the OCIO did not provide evidence of a documented and tested emergency management program.

These activities are important because many government programs rely on the resources of other agencies to fulfill their missions. According to the NCIAO's "Practices for Securing Critical Information Assets" and NIST's "Generally Accepted Principles and Practices for Securing IT Systems," the establishment of an emergency management program should focus on achieving two goals. First, minimizing known vulnerabilities associated with the most critical assets and infrastructure dependencies in an expeditious and cost-effective manner, and second, institutionalizing procedures designed to ensure timely continuation of operations of critical functions in the event of disruptions. In addition, 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.

Recruitment, Education and Awareness

Although the OCIO has made improvement in this area, the OCIO still has not fully implemented its plans for recruitment, education, and awareness relating to protecting their critical cyber-based infrastructures. HUD's CIPP identified several training and awareness initiatives as part of its entity-wide security program. Specifically, the CIPP stated the OCIO would develop a training and awareness program for mortgage and banking industry staff, perform an analysis to identify staff and contractor training requirements, use network video broadcasts to deliver security awareness and risk management training and annual refresher training, and establish a monitoring system to determine the effectiveness of its training program. During our evaluation, we found that the OCIO completed a training requirement analysis, conducted a security awareness training/conference and awareness month, and established an internal security web page. In addition, the OCIO recently awarded a contract for the development and implementation of a security and awareness-training program to include video broadcast for primary field offices, and provide risk management and security awareness and refresher training courses. However, the remaining activities outlined in the CIPP were delayed or cancelled.

Recruitment, education, and awareness are all necessary to the successful implementation of any information security program. The GISRA requires that the OCIO's security program include security awareness training to inform personnel of information security risks associated with the activities of personnel; and responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks. 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 application.

Progress Hampered by Inadequate Funding and Planning, and Administrative Processes

Delayed implementation of corrective actions and program enhancements are the result of funding limitations, poor planning and coordination, and failure to establish contractual agreements in a timely manner. As a result, progress toward strengthening HUD's agency-wide security program has been hampered and the security program remains immature thereby not fully effective in ensuring the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets. The OCIO cannot ensure protection of HUD's IT resources from fraud, loss, sabotage, or other malicious acts when planned information security initiatives are initiated and completed in a timely manner.

During our audit, we obtained and examined budget requests and budget analysis reports to determine whether OCIO adequately planned for and obtained funding for these activities. We reviewed the OCIO's "Critical Infrastructure Protection Support Capital Asset Plan and Justification - OMB Exhibit 300B," prepared as part of the annual budget process as prescribed in OMB Circular A-11. We also reviewed the "Exhibit 300Bs" dated November 16, 2000 and March 2002. We found that as part of its Critical Infrastructure Protection Support project, the OCIO reported the following two risk mitigation baseline activities in FY 01: (1) "OMB Circular A-130 Reviews and Security Assessments" and (2) "HUD's Infrastructure Security Review-

Penetration Testing, COOPs (Continuity of Operations)," at a cost of $500,000 each (See Table 1 for a list of subtasks associated with these activities).

Although OCIO officials state they have cancelled these activities, OCIO budget reports indicate that Task 1 was 100% complete as of January 31, 2002. However, we found that this initiative as planned is not complete. According to OCIO officials, under this initiative they completed OMB A-130 risk analyses for the general support system at HUD headquarters, the HUD Computer Center and the Disaster Recovery Facility as well as penetration testing for the Wide Area Network. None of the facilities (including the ASCs) received OMB-A130 reviews, (Table 1: Task 1 Subtasks). OCIO officials stated that planned OMB A-130 reviews of 40 application systems during fiscal year 2003 will replace the planned subtasks currently listed under Task 1 in Table 1. Further, Task 2, funded at $300,000, is reportedly 75% complete as of May 30, 2002 (See Table 2). OCIO officials attribute delays in implementation of planned corrective actions to the Department's mandate to develop performance-based statements of work, unexpected procurement workloads, and competing priorities for available funding. Despite cancellation of several subtasks under this initiative, the OCIO reported a cost overage of $367,000 for Activity 1 (See Table 2).

1. **Conduct OMB Circular A-130 Reviews and Security Assessments**: • FHA Data Center in Silver Springs, MD. • Copyright License Compliance • CFO Finance Center in Fort Worth, TX. • Employee Services Center in Chicago, IL. • Home Ownership Center (HOC) • 6 ITD Organizations • Administrative Service Centers (ASC's) • Personnel Security and Clearances
2. HUD's Infrastructure Security Review-Penetration Testing, COOPs: • Novell Environment • Unisys Environment • Hitachi Environment • Windows NT • AS-400

Table 1: OMB Baseline Activities (Exhibit 300B – Nov. 2000 & March 2002)

After reviewing the OCIO's budget documents, comparing planned against actual accomplishments and discussions with OCIO officials, we conclude that the OCIO cancelled performance of the ASC risk assessments as well as the review of other facilities due to inadequate funding, poor planning and coordination, and failure to establish contractual agreements in a timely manner. The OCIO must strengthen its program to ensure prompt correction of security weaknesses noted during independent and internal reviews of its information systems. In addition, the OCIO should expand the self-assessment program to include review and verification of a sample of the self-assessments completed by program

officials. In order to accomplish the objectives of its CIPP, the OCIO must promptly allocate adequate resources and mandate timely completion of initiatives outlined it the plan.

FY 2003 Exhibit 300 - Planned versus Actual Cost and Schedule Template

General Instructions: Fill in the actuals (columns F - I). Data in columns B through E reflects your Original Baseline (section B-1 of on the annotated revision). Cells F - I are the only ones available for data, as the planned numbers (Columns B - E) have been locked. Please reference the note (denoted by a red triangle) at the top of each of the actual columns for specific data entry instructions. Additional instructions are available in the FY 2003 Exhibit 300 Guidebook. ***All costs should be listed in thousands.***

	Planned				Actual			
Description	Schedule		Duration	Planned Cost	Schedule		Percentage Complete	Actual Cost
	Start Date	End Date	Days		Start Date	End Date		
1. Conduct A-130 Reviews and Security Assessments Including GISRA	02/01/00	09/30/01		$500	08/30/01	01/31/02	100%	$867
2. HUD's Infrastructure Security Review - Penetration Testing, COOPs	02/01/01	05/01/01		$300	06/15/01	05/30/02	75%	$269
3. HUD's Security Conference at Headquarters	07/01/01	07/31/01		$400	05/01/01	08/31/01	100%	$1,763
4. HUD's E-gov Security Program	02/01/01	04/01/01		$500				$0
5. Security Architecture and SDM	01/01/01	02/01/01		$50				$0
6. HUD's Security Management and Technical Support Center - Secuirty Help Desk - Monitoring and Reporting Hackers - Incident Response Program	01/01/01	09/30/01		$800				$0
7. 300 Application Security Plans and Certification and Tracking Mechanism	01/01/01	06/01/01		$400				$0
8. Study - Reston, VA. Hotsite	02/01/01	03/01/01		$100				$0
9. Security Quality Assurance and Independent Assessment - Implementing OIG and GAO findings and security best practices	01/01/01	06/01/01		$300				$0
10. Field Business Resumption Plans - formulate, review, test, and update	02/01/01	09/30/01		$200				$0
11. CIAO Project Matrix Assessment, Milestones and schedule plan	01/01/01	05/01/01		$375				$0
12. Security Tools and Products (COTS) - Hardware, Software, Physical Devices, etc/	01/01/01	09/30/01		$265				$0
13. Access Controls, Firewalls, Intrusion Detection and Monitoring, Authentication, PKI, Digital Signatures, Smart Cards, and Other Security Technologies	03/01/01	09/30/01		$225				$0
14. Security Program Management Activities - Policies and provide technical operational security support services for HUD's infrastructure.	10/01/00	09/30/01		$500				$0
15. Management Control	10/01/00	09/30/01		$373	10/01/00	09/30/01	100%	$373
16. External Reporting	10/01/00	09/30/01		$453	10/01/00	09/30/01	100%	$453
Cost Variance:	-158%							
Schedule Variance:	-77%			$5,741				$3,725

Table 2: OCIO CIP Program Budget Variance Analysis

AUDITEE COMMENTS

The Assistance Secretary for Administration/CIO provided comments to our draft in a memorandum dated September 30, 2002 (Appendix A).

OIG EVALUATION OF AUDITEE COMMENTS

After reviewing our draft audit memorandum, OCIO officials concurred with recommendation 1A and 1C. However, they did not concur with recommendation 1B. The OCIO states that OMB guidance does not require the testing and validation of the self-assessment questionnaire and that they are unaware of any other criteria that require a review the questionnaires. We continue to believe, as stated in our report, that the results of system the self-assessments have limited value in the absence of a review process to ensure responses are reasonable and complete. In addition, we believe that establishment of a review process would facilitate the OCIO taking a more active role in the self-assessment program and the analysis and reporting of results. At a minimum, the OCIO should review a sample of the self-assessments are properly completed. HUD program officials participating in the self-assessment process would also benefit from the OCIO's review of the self-assessments, as the resulting dialog and feedback would lead to increased understanding and improved proficiency in the performance of future evaluations.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1A. Proactively monitor and oversee the information security program and ensure that security weaknesses noted during independent and internal reviews of program specific systems are effectively corrected.

1B. Implement a review process to ensure the reliability of results derived from the NIST self-assessments - at a minimum review and validate a sample of the results.

1C. Ensure adequate resources are requested to enable successful implementation of the Entity-wide Security Program Plan as outlined in the CIPP.

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

SEP 30 2002

OFFICE OF THE ASSISTANT SECRETARY
FOR ADMINISTRATION

MEMORANDUM FOR: Mark C. Kaskey, Acting Director, Information Systems Audit Division, GAA

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

SUBJECT: Draft Audit Memorandum-Annual Evaluation of HUD's Information Security Program

This is in response to your draft audit memorandum, Annual Evaluation of HUD's Information Security Program, dated September 6, 2002. My staff has reviewed the subject memorandum, and concurs with recommendations 1A and 1C.

With regard to recommendation 1B, we do not concur. OMB guidance, issued July 2, 2002, for reporting the results of annual security reviews and evaluations required by the Government Information Security Reform Act, does not require the testing and validation of the self-assessment questionnaire. Also, we are not aware of any other criteria that require this proposed testing and validation. However, we do plan to test security of applications against the security plan as part of our test center practices. The current process is already very time consuming, with over 200 questions to address for each application system. Implementing recommendation 1B will only overburden our already limited staff resources and will not enhance our security program. Our time and effort would be much better spent on resolving known IT security issues rather than to continually review the questionnaire for all of HUD's application systems.

Should you or your staff have any questions, please call Donna Eden or Ken Moreau at (202) 708-2374.

DISTRIBUTION OUTSIDE OF HUD

The Honorable Joseph Lieberman, Chairman, Committee on Government Affairs
The Honorable Fred Thompson, Ranking Member, Committee on Governmental Affairs
Sharon Pinkerton, Senior Advisor, Subcommittee on Criminal Justice, Drug Policy & Human Resources
Andy Cochran, House Committee on Financial Services
Clinton C. Jones, Senior Counsel, Committee on Financial Services
Kay Gibbs, Committee on Financial Services
Stanley Czerwinski, Director, Housing and Telecommunications Issues, U.S. GAO
Steve Redburn, Chief Housing Branch, Office of Management and Budget
Linda Halliday, Department of Veterans Affairs, Office of Inspector General
William Withrow, Department of Veterans Affairs, OIG Audit Operations Division
George Reeb, Assistant Inspector General for Health Care Financing Audits
The Honorable Dan Burton, Chairman, Committee on Government Reform
The Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform