Issue Date
September 27, 2002
Audit Case Number
2002-DP-0002

TO: Vickers B. Meadows, Assistant Secretary for Administration, A

//SIGNED//

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

SUBJECT: Audit Memorandum Report - Review of Departmental IT Security Plans

INTRODUCTION

We have completed a review of security plans prepared for HUD's mission critical systems. This review was made in conjunction with the OIG's FY 2001 Financial Statement Audit and as part of the OIG's annual independent evaluation of the overall effectiveness of HUD's security program as required by the Government Information and Security Reform Act (GISRA). The objective was to determine whether security plans prepared for HUD's critical information systems were compliant with OMB Circular A-130 and consistent with National Institute of Standards Technology Publication (NIST) 800-18. We performed our audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). We limited the scope of review to evaluating security plans for five HUD mission critical financial application systems out of 54 mission critical systems identified. These five application systems were selected because they represent the major financial systems for the Department. The five systems selected for review were HUD's Centralized Accounting and Program System (HUDCAPS), Letter of Credit Control System (LOCCS), Program Accounting System (PAS), Loan Accounting System (LAS), and Community Planning and Development (CPD) Integrated Disbursement and Information System (IDIS) and were selected as a result of work performed during the annual financial statement audit. We also obtained and reviewed relevant documentation to include contractor review reports, HUD Critical Systems' Plan of Action & Milestones Report Summary, and applicable guidance and directives. We met with key personnel and conducted interviews to determine the extent of their involvement in the security planning process and the development of security plans. We performed our audit fieldwork in November 2001 and from February to May 2002.

We have received your response to the recommendations in the draft report (See Appendix A). Your office has reviewed the findings and recommendations and concurs with each

recommendation in the report. We have reviewed the proposed corrective actions and determined that they have adequately addressed our recommendations and, therefore, no further response is required. In accordance with HUD Handbook 2000.06 REV-3, we will record management decisions for the recommendations, and their respective target completion dates, in the Departmental Automated Audits Management System (DAAMS) effective September 27, 2002. We plan to monitor the progress of the implementation of these recommendations as part of our audit follow-up process.

We appreciate the assistance your staff has provided to us during the course of the review. Should you or your staff have any questions, please contact me at 202-708-0614, extension 8148.

SUMMARY

Our review found that the security plans for mission critical systems did not meet the requirements or guidelines of either OMB Circular A-130 or NIST Publication 800-18. Also, HUD has not updated the Department's information security policies and procedures for preparing security plans to conform to current OMB Circular A-130 and NIST Publication 800-18 guidelines. Additionally, the Office of the Chief Information Officer (OCIO) was not coordinating and sharing with the responsible Program Area Officials the results of a contractor's review of the Department's security plans for appropriate corrective action. Without adequate security plans and proper coordination between the OCIO and the Program Areas, the Department is at risk that critical information systems will not be adequately protected against waste, loss, and unauthorized use.

BACKGROUND

The Department of Housing and Urban Development is responsible for mission critical information systems that collectively process billions of dollars worth of transactions. Additionally, these systems are part of a network which HUD employees and contractors are dependent on to accomplish the Department's mission of insuring loans, processing subsidies and grants, and monitoring performance of its business partners. Because of the criticality of these systems it is especially important to ensure that they are properly protected through adequate security planning. Every Federal agency is required to implement and maintain a security program that ensures that all information collected, processed, transmitted and, or disseminated is protected commensurate with the harm that could result if the data was lost or misused. OMB Circular A-130 Transmittal Memorandum 4 dated November 2000, Security of Federal Automated Information Resources, requires that agencies incorporate a security plan that is compliant with Appendix III of the circular and that the plans be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Appendix III of OMB Circular A-130, establishes a minimum set of controls to be included in Federal information security programs. NIST Publication 800-18 establishes guidance on how these security controls should be represented in the agency's security plans.

Adequate security planning is critical to the success of a security program. A security plan is the essential documentation of the security requirements of a system and describes the controls in place or planned for meeting these requirements. The security plan should also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system including system owners, the system operator, and the system security manager. The system owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. The program areas within HUD are usually considered "system owners" as they are the primary users of the Departmental automated information systems.

FINDING: Significant Improvements and Better Coordination are Needed in the Management and Maintenance of HUD's System Security Plans

HUD's Security Plans are Non-Compliant with Federal Regulations and Guidelines. OMB Circular A-130 requires agencies to develop a security plan that is compliant with Appendix III of the circular and that the plans are consistent with guidance set forth in NIST Publication 800-18. OMB Circular A-130 requires that security plans contain: (1) detailed information regarding contingency planning, (2) management controls for personnel security, (3) application specific rules of behavior for users, (4) technical controls within the system, (5) appropriate protections of information shared with or obtained from other applications, and (6) public access controls when applicable.

We reviewed the system security plans for five critical HUD financial systems: HUDCAPS, PAS, LOCCS, LAS and IDIS. We found that the plans did not meet the requirements of OMB Circular A-130 and the guidelines of NIST Publication 800-18. For example, none of the system plans that we reviewed contained (1) system specific rules of behavior for users, (2) specific system information regarding interconnectivity and information sharing, (3) specific requirements for information regarding the operational and technical controls for the systems, (4) information on security reviews or risk analyses which are required to be performed at least every three years, and (5) a section that describes the public access controls used to protect system integrity and the confidence of the public in the application or why these controls are not applicable.

Security plans are essential to protect vital Information Technology (IT) resources. Without adequate security plans, HUD's critical IT resources are at risk from fraud, user errors, loss of data as well as from sabotage and other malicious acts.

HUD Issued Guidance Needs Updating. HUD Handbook 2400.24 REV-2, "Information Security Program" dated November 1999, paragraph 4-2.k states that system owners are required to develop application security plans following OMB Circular A-130, current NIST guidance, and HUD Handbook policy. Appendices G and H of the HUD Handbook contains guidance and instructions for preparing the application and general support systems security plans, respectively. However, the Appendices

reference OMB Circular A-130 of February 8, 1996 and NIST "User Guide for Developing Security Plans for Unclassified Information Systems" which have since been superseded by an updated OMB Circular A-130 and NIST Publication 800-18. As a result, we found that the Appendices lacked key guidance information as identified in NIST Publication 800-18 and contributed to the security plan deficiencies identified above.

For example, Appendix G instructions for Major Application Systems did not provide a section describing public access controls as identified in NIST Publication 800-18. This information is crucial as it details the additional security controls used to protect system integrity and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records, access controls to limit what the user can read, modify, or delete, and controls to prevent public users from modifying information on the system. We also found that Appendix G instructions for various sections did not provide the level of detail as provided in NIST Publication 800-18. For example section III.A describes the risk assessment and management as crucial elements of the security planning process but fails to mention that the security plans should also describe the risk assessment methodology used, the date the review was conducted or, if no risk assessment was performed, to include a milestone date for completion of the assessment. Such guidance is specifically addressed in the current NIST Publication 800-18 but was missing from Appendix G.

We also noted similar deficiencies when comparing current NIST guidance with the General Support Systems security plan instructions provided under Appendix H of the Handbook. For example, the Appendix did not address incident response capabilities, a critical component of a security plan for general support systems. NIST Publication 800-18 provides that the security plan should have procedures for reporting incidents handled either by system personnel or externally, procedures for recognizing and handling incidents, and what files and logs should be kept and who to contact and when.

Providing current and complete guidance to system owners is critical for preparing security plans. Without this guidance, HUD is at risk that the plans prepared by the system owners would not provide the necessary information to adequately protect the Department's critical information system resources.

Better Coordination is Needed Between the OCIO and Program Offices. The OCIO is responsible for managing the Department's information security program, to include coordinating with the Program Offices in the preparation and maintenance of their system security plans in accordance with OMB Circular A-130. The OCIO issued a memorandum, dated August 14, 2001, requesting that Program Area Officials appoint a Senior Security Manager to work closely with OCIO staff in implementing HUD's Information Systems Security Program. One of the duties of the Senior Security Manager would be to update security plans for information systems under their purview. Additionally, the OCIO engaged a contractor to perform a review of 182 systems security plans for compliance with OMB Circular A-130 and NIST Publication 800-18. On October 1, 2001, the contractor issued a final report on their review and found numerous

deficiencies with the security plans, including similar deficiencies that were found in our review of the five critical system plans. The OCIO is currently in the process of hiring a contractor to re-write the HUD system security plans to conform to OMB Circular A-130 and NIST Publication 800-18 guidelines with a planned date of April 2003 for completion.

Although the OCIO has initiated actions to address the deficiencies with the system security plans, we found the OCIO has neither provided the results of the contractor review to the Program Offices nor involved them in the resolution of the deficiencies. In discussion with various program staff, they explained that they had not received a copy of the contractor's report and were unaware of the OCIO's plans to have the system security plans re-written by a contractor. The OCIO staff informed us that the reason for not providing the Program Offices with a copy of the report or involving them in the resolution process was because they considered the contractor's report an internal OCIO document to be used to measure the Department's progress in meeting GISRA requirements. However, we do not agree with the OCIO's decision to exclude the Program Offices in the system plans resolution process. NIST Publication 800-18 provides that the system owners (Program Offices) are responsible for preparing and implementing their respective security plans and to monitor their effectiveness. Additionally, the OCIO's decision contradicts the OCIO's August 14, 2001 memorandum to the Program Offices instructing them to work closely with OCIO staff in implementing HUD's Information System's Security Program which includes updating the Department's system security plans. We believe it is critical that the OCIO coordinate with the Program Offices in the preparation and updates of system security plans to ensure they are complete and comply with OMB Circular A-130 and NIST Publication 800-18 guidelines.

AUDITEE COMMENTS

Your office has reviewed the findings and recommendations and concurs with each recommendation in the report (See Appendix A).

OIG EVALUATION OF AUDITEE COMMENTS

We have reviewed the proposed corrective actions and have determined that they have adequately addressed our recommendations.

RECOMMENDATIONS

We recommend that the Assistant Secretary for Administration, as the Departmental Chief Information Officer (CIO):

1A. Revise Appendix G and Appendix H of HUD Handbook 2400.24 and other security-related guidance to conform to the current requirements and guidelines of OMB Circular A-130 and NIST Publication 800-18.

1B. Coordinate with the Program Offices, as the system owners, to ensure (1) the Program Offices prepare and update their system security plans to correct the deficiencies identified in the contractors review and, (2) that the security plans meet all of the requirements and guidance of OMB Circular A-130 and NIST Publication 800-18.

1C. Coordinate with the Program Offices in all future reviews of system security plans to ensure that they are involved in the resolution process of any deficiencies identified.

1D. Develop an action plan to address the system security plan deficiencies identified in the contractors review. This action plan should define the roles and responsibilities for the resolution of the deficiencies along with target dates for corrective action.

APPENDIX A

Office of Administration's Comments

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

SEP - 6 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, A

SUBJECT: **INFORMATION**--Draft Audit Memorandum Report – Review of Departmental IT Security Plans, dated August 6, 2002

This is in response to your subject audit memorandum report, dated August 6, 2002. My office has reviewed the findings and recommendations and has attached a proposed Corrective Action Plan, which addresses each of the recommendations.

If you need additional information or have any questions regarding our response, please contact Ken Moreau on 708-2374.

Attachment

OCIO' Corrective Action Plan to Recommendations In OIG's
Audit Memorandum, Review of Departmental IT Security Plans (August 6, 2002)

Recommendations from the OIG Memorandum	Program Management Response
1A. Revise Appendix G and Appendix H of HUD Handbook 2400.24 and other security-related guidance to conform to the current requirements and guidelines of OMB Circular A-130 and NIST Publication 800-18.	**1A. ECD: 09/30/03 POC: Holloway Coats** OCIO concurs with this recommendation. **Planned Corrective Actions**: OCIO will procure technical security support to revise the applicable security procedures to conform to OMB Circular A-130 and NIST Publication 800-18. A Project Plan to perform this effort will be developed by 10/31/02. The estimated completion date to deliver the work identified in the Project Plan is **9/30/03**.
1B. Coordinate with the Program Offices, as the system owners, to ensure (1) the Program Offices prepare and update their system security plans to correct the deficiencies identified in the contractors review and, (2) that the security plans meet all of the requirements guidance of OMB Circular A-130 and NIST Publication 800-18.	**1B. ECD: 09/30/03 POC: Holloway Coats** OCIO concurs with this recommendation. **Planned Corrective Actions**: OCIO will procure technical security support to address the system security plan deficiencies identified in the contractor's review. A Project Plan for performing system reviews and a process for collaborating with the Program Offices, to ensure they prepare and update their system security plans to conform to OMB Circular-A130 and NIST Publication 800-18, will be developed by 10/31/02. The estimated completion date to implement the Project Plan is **9/30/03**.
1C. Coordinate with the Program Offices in all future reviews of system security plans to ensure that they are involved in the resolution process of any deficiencies identified.	**1C. ECD: 11/29/02 POC: Holloway Coats** OCIO concurs with this recommendation. **Planned Corrective Actions**: A Project Plan for system reviews, which will incorporate the involvement of the Program Offices, will be developed and published by **11/29/02**. This Project Plan will ensure that all reviews beginning in FY03 will include Program Offices.

OCIO' Corrective Action Plan to Recommendations In OIG's
Audit Memorandum, Review of Departmental IT Security Plans (August 6, 2002)

1D. Develop an action plan to address the system security plan deficiencies identified in the contractors review. This action plan should define the roles and responsibilities for the resolution of the deficiencies along with target dates for corrective action.	**1D. ECD: 11/29/02 POC: Holloway Coats** OCIO concurs with this recommendation. **Planned Corrective Actions**: OCIO will procure technical security support to address the system security plan deficiencies identified in the contractor's review, including an Action Plan that will define the roles and responsibilities for the resolution of the deficiencies along with the target dates for completion of corrective actions. Development of the Action Plan will involve close collaboration and joint decisions from both the program area and OCIO. Procurement of the technical security support, and development of the Action Plan should be completed by **11/29/02.**

DISTRIBUTIONS OUTSIDE OF HUD

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, Room 212,
O'Neil House Office Bldg., Washington, DC 20515
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
Linda Halliday, Department of Veterans Affairs, Office of Inspector General
810 Vermont Ave., NW, Washington, DC 20420
William Withrow, Department of Veterans Affairs, OIG Audit Operations Division
1100 Main, Rm 1330, Kansas City, Missouri 64105-2112
George Reeb, Assistant Inspector General for Health Care Financing Audits
N2-25-26, North Bldg., 7500 Security Blvd., Baltimore, MD 21233-1859
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
The Honorable James T. Walsh, Chairman, Subcommittee on VA, HUD,
and Independent Agencies, Committee on Appropriations House of Representatives,
Washington, DC 20515-6022
The Honorable Alan B. Mollohan, Ranking Minority Member, Subcommittee on VA,
HUD, and Independent Agencies, Committee on Appropriations, House of
Representatives, Washington, DC 20515-6022
Andy Cochran, House Committee on Financial Services, 2129 Rayburn H.O.B
Washington, DC 20515
Clinton C. Jones, Senior Counsel, Committee on Financial Services, U.S. House of
Representatives, B303 Rayburn H.O.B., Washington, DC 20515