audit report

Issue Date:
August 31, 2006
Audit Report Number
2006-DP-0005

TO: Lisa Schlosser, Chief Information Officer, A

FROM: Hanh Do, Director, Information System Audit Division, GAA

SUBJECT: Review of HUD's Information Technology Contingency Planning and Preparedness

HIGHLIGHTS

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development's (HUD) information technology contingency planning and preparedness compliance with federal requirements and its ability to recover its mission-critical and major applications, equipment, and services in the event of interruption or disaster in a timely manner. We also evaluated (1) the adequacy of the contingency planning process in developing the contingency plans for major applications and disaster recovery plans for HUD's information technology infrastructure, (2) whether the contingency planning process provided HUD with the ability to restore data in a timely manner, and (3) the adequacy of the contingency and disaster recovery plans. We performed this audit in conjunction with our ongoing audit of HUD's fiscal year 2006 consolidated financial statements.

What We Found

HUD has made significant progress in implementing information technology contingency planning and preparedness. However, our review noted several areas of concern that require management attention: (1) the current information technology contingency planning process does not fully use the planning process as recommended by the National Institute of Standards and Technology; (2) there is no assurance that the alternate data recovery facilities have the capability to restore HUD's mission-critical and major applications within the required timeframes; and (3) HUD's information technology contingency and disaster recovery plans are not documented and maintained to reflect current conditions to ensure their effectiveness in the event of a disaster.

What We Recommend

We recommend that the Office of the Chief Information Officer

- Request that program officials complete the business impact analyses (BIA) and the risk assessments and ensure that they are incorporated into HUD's contingency and disaster recovery plans and that the documents reflect current conditions and incorporate corrective actions identified through testing.

- Ensure that key Lockheed Martin personnel at its Network Operating Center in Lanham, Maryland, develop a memorandum of understanding with its alternate recovery facility that will include provisions for the (1) inclusion of disaster recovery documents at the alternate recovery sites, (2) technical support for Lotus Notes, and (3) inclusion in the alternate site's contingency plans.

- Evaluate the Electronic Data Systems (EDS) and SunGard "no priority of service" provisions to determine whether conflicting priorities impact the recovery time objectives by (1) testing the plan's ability to restore data in the required restoration time at an additional site and (2) adjusting priority access.

- Direct the information technology contingency planning coordinator to evaluate the reciprocal agreements (i.e., memorandum of understanding and service-level agreements) to ensure that the information is current and continues to meet system requirements adequately.

Auditee's Response

The complete text of the auditee's response, along with our evaluation of that response, is included in appendix A of this report.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

The U.S. Department of Housing and Urban Development's (HUD) information technology infrastructure includes two data centers, one maintained by Electronic Data Systems (EDS), located in Charleston, West Virginia, and another maintained by Lockheed Martin Corporation, located in Lanham, Maryland. Reliance on information technology has increased, and HUD depends on 111 major applications,[1] which support its major functions, business partners, and clients. Consequently, the continuity of support of the applications and recovery of information and data in the event of disaster or interruption are of great importance.

Downtime of the agency's information can become costly. A study by KPMG[2] states that 25 percent of the government participants said that it costs their agency $50,000 to $100,000 per hour for their systems to be down. In fact, one agency's system owner indicated that the downtime of just 24 hours would cost his office at least $2 million per day in tax liabilities plus additional costs incurred by clients, overtime costs, and penalties.

National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology (IT) Systems," provides instructions, recommendations, and considerations for government information technology contingency planning. It identifies fundamental planning and provides guidance to help personnel evaluate information systems and operations to determine contingency requirements and priorities. The guidance also provides a structured approach to aid planners in developing cost-effective solutions that accurately reflect their information technology requirements and integrate contingency planning principles into all aspects of information technology operations.

The objective of our audit was to assess HUD's compliance with applicable federal requirements as well as its ability to ensure that the agency can perform its major functions in a timely manner in the event of interruption or disaster. We evaluated 1) the adequacy of the contingency planning process in developing the contingency plans for major applications and disaster recovery plans for HUD's information technology infrastructure, (2) whether the contingency planning process provided HUD with the ability to restore data in a timely manner, and (3) the adequacy of the contingency and disaster recovery plans.

We used the recommendations in National Institute of Standards and Technology Special Publication 800-34 as criteria. We also used Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources" and National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," as criteria.

[1] A major application is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[2] In 2005, Continuity Insights Magazine and KPMG Risk and Advisory Services conducted a business continuity management benchmark study exploring downtime and cost of disruption. The study included 30,000 participants representing various industries reporting costs ranging from less than $50,000 to more that $5 million an hour.

RESULTS OF AUDIT

Finding 1: The Contingency Planning Process Has Improved but Deficiencies Remain

HUD's current information technology contingency planning process has not been fully implemented as recommended in National Institute of Standards and Technology Special Publication 800-34.[3] In previous years, we reported that HUD's information technology contingency planning process needed improvement. Specifically, in prior years we recommended that the agency complete business impact analyses (BIA) and risk assessments on each system. However, HUD did not incorporate the business impact analyses (BIA) in the development of the contingency and disaster recovery plans or identify preventive controls for the current information technology infrastructure. As a result, it has not identified all requirements considered necessary for restoration of its infrastructure in the event of disaster or interruption, and it has not identified all risks and controls that could mitigate the potential vulnerabilities and threats it may incur.

The information technology contingency planning process encompasses procedures designed to sustain and recover critical services following an emergency. The process includes seven key steps, which represent key elements in a comprehensive information technology contingency planning capability.

The business impact analysis (BIA)[4] is the second step in the contingency planning process. The BIA enables the contingency planning coordinator to clarify the system specifications, processes, and interdependencies and use this information to determine contingency requirements and priorities. Results from the BIA should be included in the analysis and development of the organization's suite of plans used to restore and recover the organization.

Identifying preventive controls is the third step in the contingency planning process. Risk management activities from the information technology contingency planning perspective have two functions. First, they should identify threats and vulnerabilities so that appropriate controls can be put into place. Second, they should identify risks for which contingency plans must be put into place. The contingency plan, therefore, is closely tied to the results of the risk assessment.[5]

[3] National Institute of Standards and Technology Special Publication 800-34 defines a seven-step contingency planning process: (1) develop the contingency planning policy statement; (2) conduct the business impact analysis (BIA); (3) identify preventive controls; (4) develop recovery strategies; (5) develop an information technology contingency plan; (6) plan testing, training, and exercises; and (7) plan maintenance.

[4] The business impact analysis (BIA) is central to determining what recovery strategies should be implemented to ensure availability.

[5] A thorough risk assessment should identify the system vulnerabilities, threat, and current controls and attempt to determine the risk, based on the likelihood and threat impact.

HUD Did Not Incorporate BIAs in the Development of the Contingency and Disaster Recovery Plans

HUD did not incorporate the business impact analyses (BIA) in the strategy and development of its contingency and disaster recovery plans. It has begun to develop contingency plans and conduct BIAs for its 111 major applications. However, not all program offices have completed a BIA for their respective application system. HUD has completed 46 percent (51 out of 111) of the BIAs for major application systems. Eighty-four percent of the contingency plans (93 of 111) were completed for major application systems, of which 45 percent (42 of 93) were completed without a BIA.

Our review identified instances in which the completed business impact analyses (BIA) were inadequate and the results were not incorporated in the development of the completed contingency and disaster recovery plans. For example, little or no analysis was performed in the analysis and development of the BIA for some mission-critical application systems. The BIAs referenced and used an outdated HUD Information Technology Services interim disaster recovery plan that did not reflect the current environment and recovery strategies. The completed BIAs included a list of personnel assigned to critical roles necessary to recover major application systems. However, the corresponding contingency plans did not include any of those assigned staff.

Preventive Controls Have Not Been Identified for HUD's Current Information Technology Infrastructure

HUD has not identified preventive controls for the current information technology infrastructure. To effectively determine the specific risks to an information technology system during service interruption, a risk assessment of the system environment is required. An Office of Inspector General (OIG) audit during fiscal year 2005[6] determined that none of the 50 major application systems' risk assessments reviewed reflected the change in location of HUD's data centers or change in risk profile that resulted in the hardware platforms operating system software ownership shifting from HUD to a contractor as part of HUD's new infrastructure contract. The risk assessments conducted revealed a common pattern of deficiencies, to include minimal technical evaluation of security controls, gaps, and inaccuracies in the text.

[6] Audit Report 2006-DP-0004, "Review of HUD's Information Security Program," dated February 14, 2006.

Conclusion

HUD has not identified all of the requirements considered necessary for restoration of its infrastructure in the event of disaster or interruption. It has also not identified all risks and preventive controls that could mitigate the potential vulnerabilities and threats it may incur. Not all of the system owners conducted a business impact analysis (BIA) for their respective systems. Additionally, none of the 50 major application systems' risk assessments reviewed by OIG during fiscal year 2005 reflected the current information technology infrastructure. Further, the results from the BIAs and risk assessments were not appropriately incorporated into the analysis and strategy development efforts for the organization's contingency and disaster recovery plans. Without effective contingency planning, HUD cannot ensure effective response, recovery, and continuity activities for disruptions affecting information technology systems, business processes, and the facility.

Recommendations

We recommend that the information technology contingency planning coordinator within the Office of the Chief Information Officer

1A. Request that program officials complete the business impact analyses (BIA) for their systems and incorporate them into the development and update of the information technology contingency plans in accordance with federal and agency requirements.

1B. Request that program officials update the risk assessments of the current information technology infrastructure and incorporate them into the development and update of the information technology contingency plans in accordance with federal and agency requirements.

1C. Review, coordinate, and ensure that the business impact analysis (BIA) requirements and current risk assessments are incorporated into the analysis, development, and modification efforts for the organization's contingency and disaster recovery plans.

Finding 2: HUD Has No Assurance That the Alternate Data Recovery Facilities Can Restore Its Data in the Required Restoration Time

Although HUD has alternate data recovery facilities that have the capability to restore its mission-critical and major applications, there is no assurance that those facilities have the capability to enable HUD to perform and restore its mission-critical and major applications within the recovery time objectives.[7] For example, (1) there is no memorandum of understanding between the Lockheed Martin Network Operating Center and its alternate data recovery facility, and (2) the HUD contractor has not made provisions that HUD data have priority over other clients' data in the event of a disaster simultaneously affecting customers.

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. These alternate sites may be owned and operated by the organization, or commercial sites may be available under contract. Regardless of the type of alternate site chosen, agreements should be established with the primary and alternate facility to ensure that the alternate facility will be able to restore the primary site's operations as defined in the agency's contingency and related plans.

Two or more organizations with similar or identical information technology configurations and backup technologies may enter a formal agreement to serve as an alternate site. This type of site is set up via an agreement or memorandum of understanding. If contracting with a commercial vendor, customers should be aware that multiple organizations may contract with a vendor for the same alternate site. As a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.

The agreements that the HUD data centers have with their respective alternate recovery facilities do not have controls in place to ensure the recovery time objectives of 24 hours for mission-critical application systems and 48 to 72 hours for major application systems as defined by the contingency and related plans.

There Is No Memorandum of Understanding

There is no memorandum of understanding between the Lockheed Martin Network Operating Center in Lanham, Maryland,[8] and its alternate data recovery facility at the Lockheed Martin Corporation in Orlando, Florida. Without a

[7] Recovery time objective is the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization.

[8] Lockheed Martin Corporation is responsible for the HUD network outside the Charleston data center and Lotus Notes electronic mail.

memorandum of understanding between the two sites, there is no agreement that addresses the types of controls that are imperative to assure the security and restoration of HUD’s mission-critical and major applications and information technology infrastructure at that site within the required timeframe.

- There are no disaster recovery plans available on site at the alternate site. A copy should be stored at the alternate site in Orlando, Florida, as well as the primary site in Lanham, Maryland.

- There are no technical support personnel on site at the alternate site in Orlando, Florida, and Lockeed Martin has not identified a remote administrator for the Lotus Notes e-mail software in the event of interruption or disaster at the Lanham, Maryland, facility.

- The contingency plans for the alternate site in Orlando, Florida, that address the recovery of operations at that site do not include recovery procedures for HUD data. Thus, in the event of disaster, there are no plans for restoring HUD data at the alternate site.

There Is No Priority of Access for HUD Data

Electronic Data Systems (EDS) is responsible for support of the IBM and Unisys mainframes and those UNIX and Windows servers currently located at the Charleston, West Virginia, data center. EDS contracted SunGard, a commercial vendor, located in Philadelphia, Pennsylvania, for its alternate data recovery facility for HUD data at the Charleston, West Virginia, data center. SunGard provides services for several EDS clients. However, SunGard does not provide priority access for its clients and will not provide an estimate of how many clients could be vying for the same resources if a disaster affects enough of those customers simultaneously. To accommodate clients when the Philadelphia site is not available, SunGard has made provisions to restore data to additional SunGard locations. However, HUD cannot determine whether SunGard can restore data at the additional alternate sites within the required recovery time objectives of 24 hours for its mission-critical applications and 48 to 72 hours for its major applications because it has not determined the impact of the additional time needed to make adjustments to redirect personnel and resources to the new location and reroute data from the Philadelphia site.

Conclusion

HUD did not review and ensure that the reciprocal agreements between the primary data centers and their respective alternate sites address security controls sufficient to ensure restoration of its mission-critical and major applications and supporting information technology infrastructure within the required timeframe. Without this agreement, there is no guarantee that HUD's systems and operations can be recovered in a timely and cost-efficient manner, thereby impacting HUD's creditability as well as its ability to provide housing to its clients. In addition, the absence of this control can result in significant downtime costs.

Recommendations

We recommend that the Office of the Chief Information Officer

2A. Ensure that Lockheed Martin Network Operating Center in Lanham, Maryland, develop a memorandum of understanding with its alternate recovery facility in Orlando, Florida, that will include the following controls:

- Ensure that disaster recovery documents (disaster recovery plan, standard operating procedures, etc.) are available at the alternate recovery facility.
- Provide for on-site technical support or provide and identify a remote administrator for the Lotus Notes e-mail application system.
- Develop a contingency plan for the Lotus Notes e-mail application system for the alternate facility in which HUD's infrastructure is included.

2B. Evaluate the Electronic Data Systems (EDS) and SunGard "no priority of service" provisions to determine whether conflicting priorities impact the recovery time objectives by (1) testing the plan to determine whether conflicting customers and relocation to another site impede the agency's ability to restore data in the required restoration time and (2) adjusting priority access to ensure that restoration of data occurs in the required time.

2C. Direct the information technology contingency planning coordinator to evaluate the reciprocal agreements (i.e., memorandum of understanding and service-level agreements) to ensure that the information is current and continues to meet system requirements adequately.

Finding 3: Documentation and Maintenance of HUD's Disaster Recovery Plans and Information Technology Contingency Plans Are Outdated

HUD's disaster recovery plans and information technology contingency plans are not updated to reflect current conditions and system enhancements. In previous years, we reported that HUD's information technology contingency planning process needed improvement. Specifically, we recommended that HUD update its information technology contingency plan to reflect current conditions and review the plan for accuracy and completeness at least annually. National Institute of Standards and Technology Special Publication 800-34 recommends that an effective plan be maintained in a ready state and accurately reflect system requirements, procedures, organizational structure, and policies. However, as reported in prior years, we found instances to the contrary.

A disaster recovery or contingency plan should be a living document that is updated regularly to remain current with system enhancements. To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure that new information is documented and contingency measures are revised if necessary.

As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews. Changes made to the plan, strategies, and policies should be coordinated through the contingency planning coordinator, who should communicate changes to the representatives of associated plans or programs as necessary. The contingency planning coordinator also should evaluate supporting information to ensure that it is current and continues to meet system requirements adequately.

The contingency planning coordinator should coordinate frequently with associated internal and external organizations and system points of contact[9] to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.

[9] Each program office head will designate a contingency planning point of contact, who will be responsible for providing the required plans and procedures.

Disaster Recovery Plans Have Not Been Updated to Reflect Current Conditions

The disaster recovery plan developed by Electronic Data Systems (EDS) for the data center facility is not current. Our review of the disaster recovery plan indicated that

- The listing of mission-critical applications is not current and has not been updated since 2003. The list does not reflect mission-critical systems that have been inactivated or added.

- The listing of recovery personnel is inaccurate. The list identifies 12 employees who have left HUD.

- The test scripts are not current and reference applications that no longer reside at the EDS data center.

- Disaster recovery test results for a test conducted in July 2005 were not analyzed and incorporated into the disaster recovery plan.

The disaster recovery plan developed by Lockheed Martin for network operations facility maintenance is not current.

- It does not contain a list of mission-critical systems that Lockheed Martin is responsible for maintaining.

- There is no documented assignment of all identified recovery roles. The disaster recovery plan identifies only four personnel assigned to the Lotus Notes electronic mail server recovery team. However, according to Lockheed Martin staff, there are 11 recovery team employees.

Contingency Plans for Major Applications Have Not Been Updated to Reflect Current Conditions

Contingency plans for major applications have not been updated by system owners to reflect current conditions, test results, and recommended corrective actions for tests conducted in September 2005. Rather, the plans continue to reference an outdated interim disaster recovery plan and continuity of operations plan.

Conclusion

The information technology contingency planning coordinator conducted a cursory review of the contingency and disaster recovery plans but did not ensure that the contingency plans were updated and incorporated mission-critical test results. The information technology contingency planning coordinator instituted a compliance review program to ensure that security documentation, to include contingency plans, are reviewed annually and that weaknesses are incorporated into the applicable system-level plan of actions and milestones.

Without effective contingency and disaster recovery plans that reflect current conditions, the plans may not be effective in the event of disruption or disaster and ensure that critical business processes are restored within a reasonable period.

Recommendations

We recommend that the information technology contingency planning coordinator within the Office of the Chief Information Officer

3A. Instruct program officials to regularly review and update contingency plans and ensure that the plans reflect current conditions and incorporate corrective actions identified through testing.

3B. Ensure that the responsible contractor regularly review and update the disaster recovery plans and ensure that the plans reflect current conditions and incorporate corrective actions identified through testing.

3C. Regularly review contingency and disaster recovery plans and coordinate with system owners and responsible contractors to ensure that the documents reflect current conditions.

SCOPE AND METHODOLOGY

We performed the audit

- From January through August 2006.
- At HUD Headquarters in Washington, DC; the Lockheed Martin data center in Lanham, Maryland; the Lockheed Martin alternate disaster recovery facility in Orlando, Florida; the Electronic Data Systems (EDS) data center in Charleston, West Virginia; the SunGard disaster recovery facilities in Philadelphia, Pennsylvania, and Warminster, Pennsylvania.
- In accordance with generally accepted government auditing standards.

Our assessment focused on the contingency planning process and preparedness conducted for HUD's major application systems in calendar year 2006.

Our review was based on the Government Accountability Office "Federal Information System Controls Audit Manual" and information technology guidelines established by the Office of Management and Budget and the National Institute of Standards and Technology. These publications contain guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data.

To accomplish our objectives, we reviewed information systems controls intended to ensure recovery of computer processing operations in case of disaster or other unexpected interruption. To evaluate these controls, we identified and reviewed HUD's policies and procedures, conducted tests and observations of controls in operation, and held discussions with HUD staff and contractors to determine whether information systems controls were in place, adequately designed, and operating effectively.

Our review included follow-up work on previous OIG recommendations that were within the scope of this audit. However, due to the limited scope of this review, limited resources, and time constraints, we did not address all previous information technology contingency planning related recommendations. Specifically, we did not follow-up on recommendations 2a, 2b, and 2c issued in the "Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audits," audit report No. 2004-DP-0001 and recommendation 5c issued in "Fiscal Year 2004 Review of Information Systems Controls in Support of the Financial Statements Audits," audit report No. 2005-DP-0001. We plan to follow-up on these recommendations under a separate OIG audit.

INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined the following internal controls were relevant to our audit objectives:

- Policies, procedures, management, and operational and technical controls used for implementing effective contingency planning processes and techniques.
- Policies, procedures, management, and operational and technical controls used for implementing contingency preparedness to restore data operations

We assessed the relevant controls identified above.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

Significant Weaknesses

Based on our review, we believe the following items are significant weaknesses:

- HUD did not have sufficient management controls over the contingency planning process to ensure that all necessary requirements had been identified for restoration and did not identify all risks and preventive controls that could mitigate the potential vulnerabilities and threats it may incur. (Finding1)
- HUD did not establish adequate controls to provide assurance that adequate restoration practices were in operation to recover information technology operations in a timely and orderly manner in the event of a disruption. (Finding 2 and 3)

FOLLOWUP ON PRIOR AUDITS

We followed up on recommendations from prior year audits and found that the following remain open:

Fiscal Year 2003 Review of Information Systems Controls in Support of the HUD Financial Statements Audit: 2004-DP-0001

2A. Adopt National Institute of Standards and Technology Special Publication 800-34, “Contingency Planning Guide for Information Technology System,” for developing contingency-related planning as follows: (a) adopt the seven steps; (b) adopt definitions for the various contingency-related plans; and (c) develop additional plans and revise current plans to address the entire suite of contingency-related plans to include the (1) business continuity plan, (2) business recovery (or resumption) plan, (3) continuity of operations plan, (4) continuity of support plan/information technology contingency plan, (5) crisis communications plan, (6) cyber incident response plan, (7) disaster recovery plan, and (8) occupant emergency plan.

2B. Ensure that contingency-related plans are updated or developed to take into consideration nontraditional disasters, such as massive regional power blackouts like the one that occurred on August 14, 2003, and terrorist strikes of the magnitude of the September 11, 2001, attacks. For example, plan assumptions and scenarios should address scenarios in which more than one facility is affected at the same time, including significant delays with respect to the availability of highways, airports, trains, buses, police, firefighters, rescue workers, and key personnel.

2C. Ensure that testing is conducted on contingency-related plans by (a) testing the continuity of operations plan at the alternate site as outlined by Federal Preparedness Circulars (FPC) 66, “Test, Training, and Exercise Program for Continuity of Operations”; (b) developing and testing a contingency plan for the transition phase, during which the workload and equipment from the current disaster recovery facility in Virginia and the data center in Maryland will be installed and migrated to the new disaster recovery facility in West Virginia; and (c) following National Institute of Standards and Technology Special Publication 800-34, “Contingency Planning Guide for Information Technology System,” by first individually testing each element of the contingency plan and then testing it as a whole to confirm the accuracy of recovery procedures and its overall effectiveness. Testing should occur at least annually and when significant changes are made to the information technology system, supported business processes, or the information technology contingency plan.

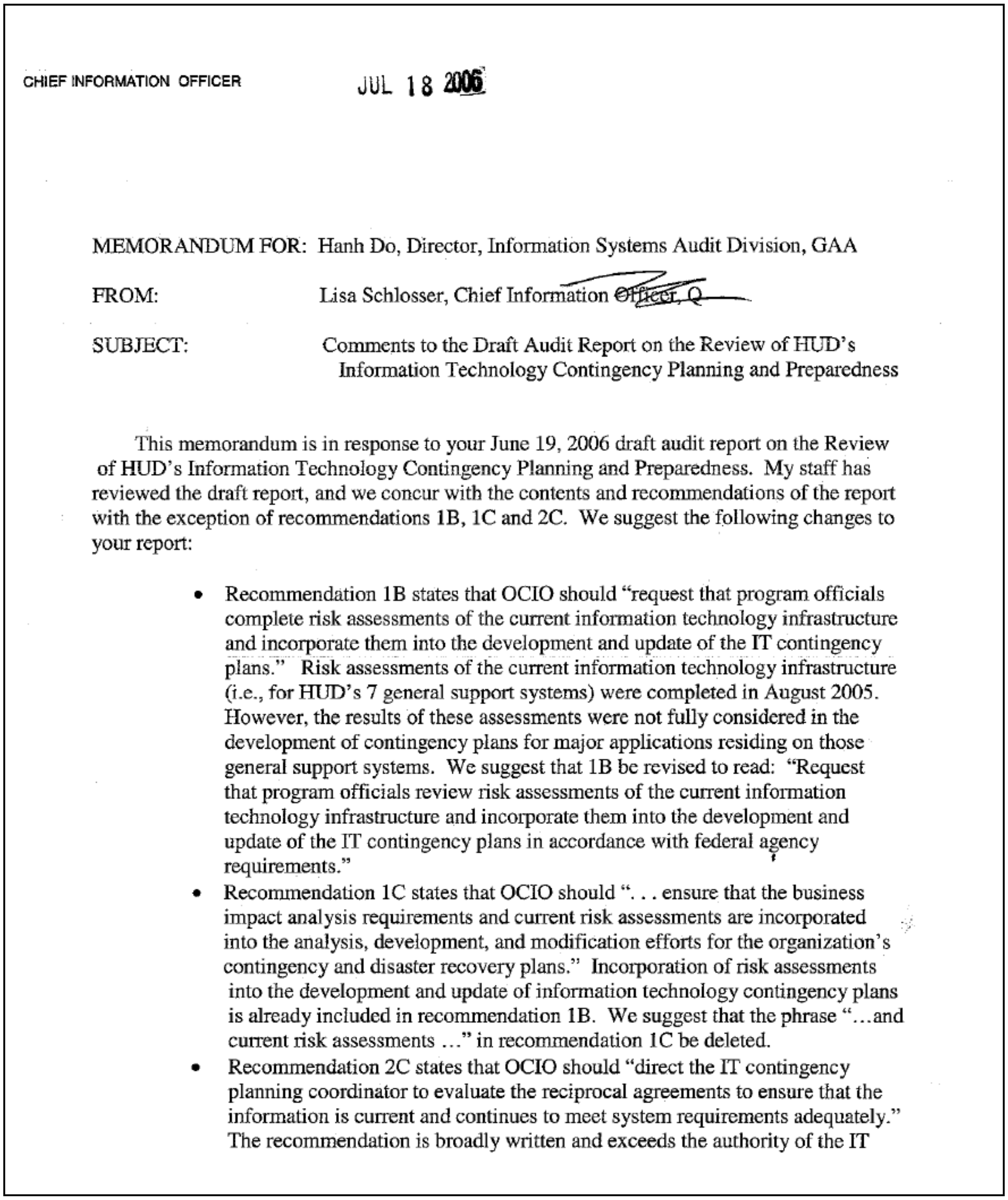
5C. Risk assessments and business impact analyses (BIA) are completed on each system.

APPENDIXES

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation **Auditee Comments**



CHIEF INFORMATION OFFICER JUL 18 2006

MEMORANDUM FOR: Hanh Do, Director, Information Systems Audit Division, GAA

FROM: Lisa Schlosser, Chief Information Officer

SUBJECT: Comments to the Draft Audit Report on the Review of HUD's Information Technology Contingency Planning and Preparedness

This memorandum is in response to your June 19, 2006 draft audit report on the Review of HUD's Information Technology Contingency Planning and Preparedness. My staff has reviewed the draft report, and we concur with the contents and recommendations of the report with the exception of recommendations 1B, 1C and 2C. We suggest the following changes to your report:

Comment 1

- Recommendation 1B states that OCIO should "request that program officials complete risk assessments of the current information technology infrastructure and incorporate them into the development and update of the IT contingency plans." Risk assessments of the current information technology infrastructure (i.e., for HUD's 7 general support systems) were completed in August 2005. However, the results of these assessments were not fully considered in the development of contingency plans for major applications residing on those general support systems. We suggest that 1B be revised to read: "Request that program officials review risk assessments of the current information technology infrastructure and incorporate them into the development and update of the IT contingency plans in accordance with federal agency requirements."

Comment 2

- Recommendation 1C states that OCIO should ". . . ensure that the business impact analysis requirements and current risk assessments are incorporated into the analysis, development, and modification efforts for the organization's contingency and disaster recovery plans." Incorporation of risk assessments into the development and update of information technology contingency plans is already included in recommendation 1B. We suggest that the phrase "…and current risk assessments …" in recommendation 1C be deleted.

Comment 3

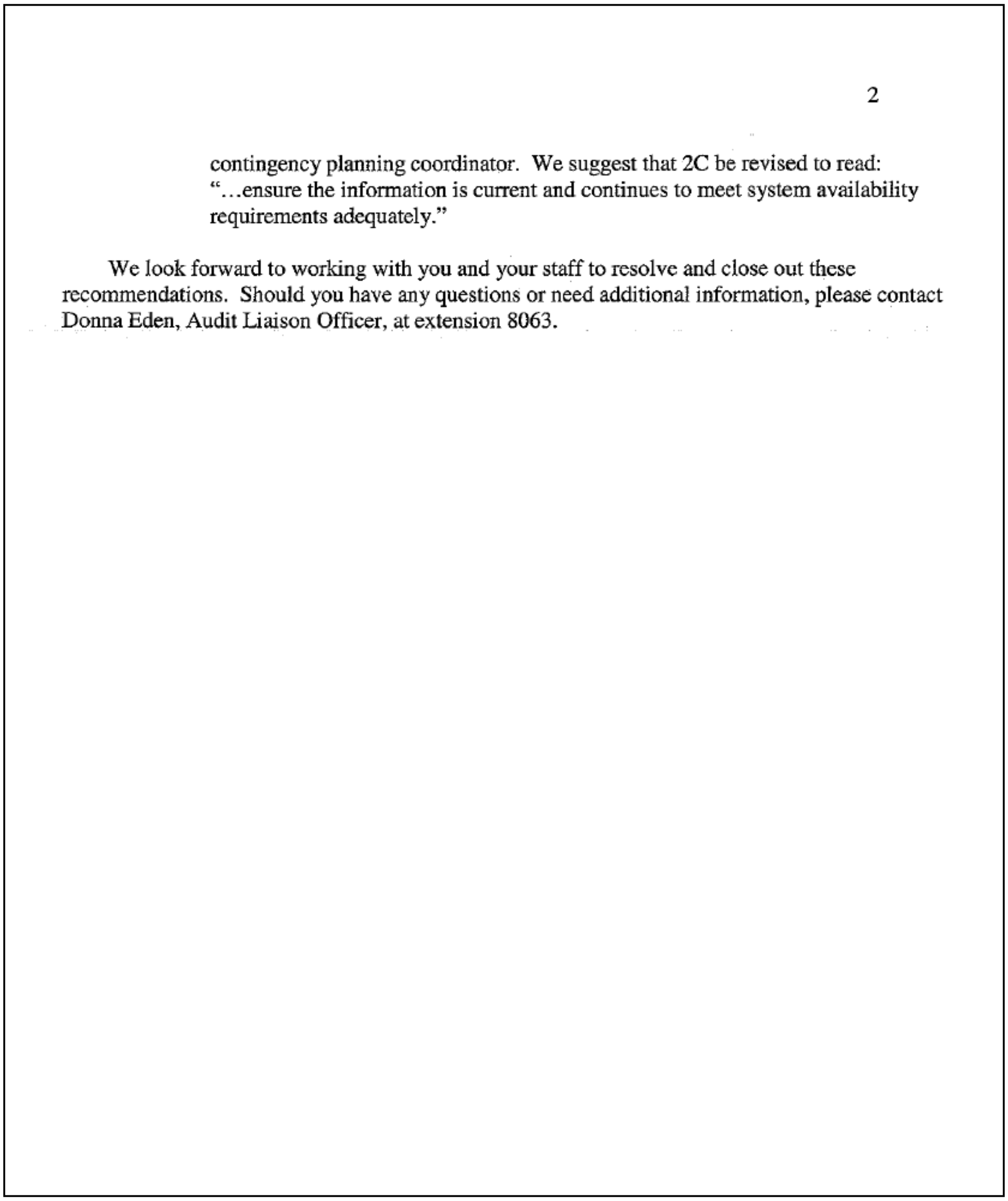
- Recommendation 2C states that OCIO should "direct the IT contingency planning coordinator to evaluate the reciprocal agreements to ensure that the information is current and continues to meet system requirements adequately." The recommendation is broadly written and exceeds the authority of the IT

APPENDIXES

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation **Auditee Comments**



contingency planning coordinator. We suggest that 2C be revised to read: "…ensure the information is current and continues to meet system availability requirements adequately."

We look forward to working with you and your staff to resolve and close out these recommendations. Should you have any questions or need additional information, please contact Donna Eden, Audit Liaison Officer, at extension 8063.

OIG Evaluation of Auditee Comments

We met with the Office of the Chief Information Officer staff to resolve their comments to the draft audit report as follows:

Comment 1 We maintain that the risk assessments are obsolete and do not reflect the current information technology infrastructure. We revised the recommendation as follows: "OCIO should request that program officials *update* risk assessments of the current information technology infrastructure...." instead of "OCIO should request that program officials *complete* risk assessments of the current information technology infrastructure...." The auditee agreed with the revision.

Comment 2 We explained to the auditee that recommendation 1C could not be deleted because it differs from recommendation 1B in that it recommends that the risk assessments should be incorporated in both the contingency plans **and** the disaster recovery plans. The auditee agreed with our decision based upon our explanation and clarification of the recommendation.

Comment 3 We explained to the auditee that the recommendation is based on the National Institute of Standards and Technology Special Publication 800-34, section 3.6, "Plan Maintenance," which requires that the contingency planning coordinator evaluate supporting information to ensure that the information is current and continues to meet system requirements adequately. Furthermore, the recommendation requests that the Chief Information Officer, who does have the authority to direct the information technology contingency planning coordinator, evaluate supporting information to ensure that the information is current and adequately continues to meet system requirements. Therefore, we would not revise recommendation 2C, as requested. The auditee agreed with our decision based upon our explanation and clarification of the recommendation.