

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Disaster Recovery Planning for DHS Information Systems Needs Improvement (Redacted)



Notice: The Department of Homeland Security, Office Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552 (b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-05-22

May 2005

*Office of Inspector
General*

**U.S. Department of
Homeland Security**
Washington, DC 20528



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared by the OIG as part of its DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report addresses the strengths and weaknesses of the DHS Information Technology disaster recovery program. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink that reads "Richard L. Skinner".

Richard L. Skinner
Acting Inspector General

Contents

Introduction.....	3
Executive Summary	4
Background.....	4
Results of Audit	7
Disaster Recovery Sites Are Inadequate.....	7
Disaster Recovery Documentation Needs Improvement.....	13
DHS Does Not Have an Enterprise-Wide Disaster Recovery Program	14
Recommendations.....	16
Management Comments and Our Evaluation.....	16

Appendices

Appendix A: Purpose, Scope, and Methodology	18
Appendix B: Management’s Response.....	20
Appendix C: DHS Facilities Reviewed	23
Appendix D: Disaster Recovery Planning Documents Reviewed	25
Appendix E: Major Contributors to This Report.....	30
Appendix F: Report Distribution.....	31

Abbreviations

BTS	Border and Transportation Security
CBP	Customs and Border Protection
CIO	Chief Information Officer
Coast Guard	United States Coast Guard
COOP	Continuity of Operations
DCC	Data Center Consolidation
DHS	Department of Homeland Security
DHS Management	DHS Management Directorate
EIB	Enterprise Infrastructure Board
FEMA	Federal Emergency Management Agency

Contents

FLETC	Federal Law Enforcement Training Center
FPC	Federal Preparedness Circular
ICE	Immigration and Customs Enforcement
IAIP	Information Analysis and Infrastructure Protection
IT	Information Technology
IV&V	Independent Verification and Validation
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
Secret Service	United States Secret Service
TSA	Transportation Security Administration

OIG

*Department of Homeland Security
Office of Inspector General*

Introduction

The Department of Homeland Security (DHS) relies on a variety of critical Information Technology (IT) systems and technologies to support its wide-ranging missions, including counter-terrorism, border security, and infrastructure protection. DHS IT systems also allow employees to communicate internally and for the American public to communicate with the department. DHS must be able to recover its IT systems quickly and effectively following a service disruption or disaster in order to continue performing these mission essential functions. This audit focused on DHS' acquisition and management of disaster recovery alternate facilities for its critical IT systems.

The Office of Inspector General (OIG) audited the IT disaster recovery capabilities for 19 DHS facilities, which were connected to the DHS network backbone.¹ The objective of this audit was to evaluate the effectiveness of DHS' acquisition and management of disaster recovery alternate facilities for the support systems processed at selected facilities. Facilities selected for this audit represented each of the DHS components,² with the exception of the Science and Technology Directorate³ and the United States Citizenship and Immigration Services.⁴ Audit fieldwork was performed in the Washington, DC area, and at several DHS locations around the country. See Appendix A for a discussion of our purpose, scope, and methodology.

¹ The 'backbone' is DHS' top-level, high-speed, data transmission telecommunications network. It serves as the major access point for telecommunications networks of DHS components.

² DHS 'components' are its directorates, including organizational elements and bureaus, and critical agencies.

³ While the Science and Technology Directorate had facilities attached to the DHS network backbone, these facilities did not have significant IT assets and were not included in the audit scope.

⁴ The United States Citizenship and Immigration Services was not responsible for a facility attached to the DHS network backbone in November 2003.

Executive Summary

DHS IT disaster recovery sites were not prepared to prevent service disruptions from potentially hindering DHS' ability to perform mission essential functions. Specifically, 15 of the 19 (79%) facilities reviewed did not have a recovery site - or the recovery site was not fully operational. Additionally, while 4 of the 19 (21%) facilities had fully operational disaster recovery sites, tests at those facilities revealed deficiencies that could adversely impact recovery of critical IT systems. The inability to restore DHS' critical IT systems following a disaster could have negative effects on the performance of mission essential functions. These potential effects include a disruption in passenger screening operations, delays in processing grants in response to a disaster, and delays in the flow of goods across U.S. borders.

Additionally, we evaluated the adequacy of disaster recovery planning documents such as continuity of operations and contingency plans. We identified deficiencies in 25 of the 31 (81%) documents reviewed. Thirteen of the 31 (42%) planning documents had not been finalized.

These problems with disaster recovery are occurring in part because DHS does not have a program in place to provide an enterprise-wide disaster recovery solution. However, DHS' Chief Information Officer (CIO) is studying the consolidation of the department's data centers. This effort could be used to provide the basis for an enterprise-wide disaster recovery capability.

We are recommending that the CIO: (1) allocate funds needed to implement an enterprise-wide disaster recovery program for mission critical systems; (2) require that disaster recovery capabilities are included in the planning and implementation of new systems; and (3) require that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards.

Background

DHS' mission includes protecting the American people and their homeland from terrorist attacks, reducing the vulnerability to terrorism, and mitigating the damage resulting from disasters, whether man-made or natural. IT assets at DHS facilities around

the country support these missions. DHS must have a disaster recovery capability in order to prevent minor disruptions or major disasters from affecting its ability to perform essential services.

IT systems can experience disruptions due to inherent vulnerabilities, such as disk drive failures or as the result of an external threat. However, even a minor disruption could become a major problem without adequate backup and recovery capability. For example, a recent problem with a private sector company's database application, combined with a manual backup system, resulted in the cancellation of hundreds of flights and disrupted the plans of thousands of traveling passengers.

The chance that a disruption may occur can be reduced through the implementation of compensatory technical or managerial controls. However, IT systems also face the risk of a service disruption caused by natural and man-made events that cannot be controlled. When there is a disruption, DHS must be able to recover its mission essential IT systems as quickly as possible. Restoring IT systems may require relocating to an alternate site if the original facility is destroyed, as occurred in the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City and the terrorist attacks on September 11, 2001. Relocating to an alternate site may be necessary if the primary facility is rendered inaccessible, as occurred when legislative and postal facilities were contaminated during the anthrax bio-terrorism attacks of 2001. Disaster recovery planning includes identifying an alternate facility that is capable of operating those IT systems if the original facility cannot be used.

Additionally, depending on the threat, the identified alternate site must be at a reasonable distance from the original facility. For example, facilities that could be subject to terrorist activities may require an alternate facility outside the metropolitan area. Facilities that are at high risk from natural disasters, such as hurricanes and earthquakes, may need an alternate facility outside their geographic region.

It is the policy of the United States to have in place a comprehensive and effective program to ensure continuity of essential federal functions under all circumstances. To support this policy, the federal government has implemented the Continuity of Operations (COOP) Program. Today's changing threat environment and the potential for no-notice emergencies, including localized acts of nature, accidents, technological emergencies, and

military or terrorist attack-related incidents, have increased the need for COOP capabilities and plans that enable agencies to continue their essential functions across a broad spectrum of emergencies. Responsibility for formulating guidance on these plans and for assessing executive branch capabilities lies with DHS' Emergency Preparedness and Response component and its Federal Emergency Management Agency (FEMA). This guidance, Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations (COOP)*, was reissued by FEMA in June 2004.

FPC 65 provides guidance on the selection of an alternate facility and requires that federal departments identify their essential functions as well as the IT systems necessary to perform these functions. Additionally, FPC 65 defines various elements which must be in a viable departmental COOP capability including:

- Implementation without warning;
- Operational within 12 hours of COOP activation;
- Regularly scheduled testing, training, and exercising of agency personnel, equipment, systems, processes, and procedures used to support the agency during a COOP event; and
- Consideration of the distance of the alternate operating facility from the primary facility.

Other government-wide guidance in this area is included in the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*. OMB Circular A-130 establishes a minimum set of controls to be included in federal automated information security programs, including the need to establish and periodically test the capability to continue providing service following a disruption to the IT system. OMB Circular A-130, at page 12 of Appendix III, emphasizes the need to test recovery plans:

“Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security.”

Additionally, the National Institute of Standards and Technology's (NIST) special publication 800-34, *Contingency Planning Guide for Information Technology Systems*, provides guidance on what

information should be in a contingency plan, and recommends that backup media should be stored off-site in a secure, environmentally-controlled location. NIST SP 800-34 also notes that the performance of a business impact analysis is a key step in the contingency planning process. This analysis helps to correlate specific system components with the essential services that they provide; and to characterize the consequences of a disruption to the system components on those essential services. The disruption impacts and allowable outage times identified help to determine the most cost-effective backup and recovery process for the system.

Also, DHS provides disaster recovery guidance to its components in its Sensitive Systems policy publication 4300A, *Information Technology Security Program*. This DHS-wide guidance for implementing disaster recovery procedures expands on FPC 65 and OMB Circular A-130 testing guidance by requiring that DHS components develop and maintain disaster recovery plans and that these plans be tested/exercised annually. DHS 4300A also provides broad guidance on the storage of backup tapes.

Results of Audit

Disaster Recovery Sites Are Inadequate

The disaster recovery sites for the reviewed DHS facilities were either not available, not fully operational, or had identified deficiencies (See Appendix C, *DHS Facilities Reviewed*, for details). The disaster recovery sites for all 19 facilities lacked adequate capabilities to prevent service disruptions from potentially affecting DHS' ability to either respond to a threat or to mitigate the effects of a disaster. Specifically, there was no identified recovery site for six of the 19 (32%) selected facilities. At these six facilities there were a total of 383 servers and nine mainframe systems.

DHS components also placed reliance on disaster recovery sites that were not fully operational at nine of the 19 (47%) facilities. There were a total of 500 servers at these nine facilities. These alternate sites were not fully operational because they did not have all the resources necessary to recover the functions at the original facility.

DHS Disaster Recovery Planning Needs Improvement

Additionally, only four of the 19 (21%) facilities, consisting of a total of eight mainframe systems and 390 servers, had operational disaster recovery sites and tested their disaster recovery planning. The disaster recovery testing at these four operational recovery sites revealed deficiencies that could adversely impact recovery of critical systems.

DHS must be able to provide mission essential services with minimal disruption following a disaster. DHS recovery sites must be able to restore promptly the critical IT systems supporting these services. Without an adequate disaster recovery capability, a minor disruption or major disaster may affect DHS' ability to perform essential services.

The impact on DHS of a disaster at one of these 19 facilities is dependent upon the duration of the failure and the importance of the IT systems operating at that facility. For example, if the facility contained mission critical systems, damage or destruction to those systems could have a debilitating impact on the ability of DHS to perform its essential functions and activities.

Component A⁵

Component A was responsible for two of the facilities without an identified disaster recovery site. The inability to access critical applications running on the 228 servers and nine mainframes at these Component A facilities could adversely impact security operations (b) [REDACTED], or delay recovery and coordination efforts to respond to an incident.

Component A is using a managed services contract to provide IT services. This contract could be used to provide a disaster recovery capability for these two facilities; however, Component A does not have the funds available to task the contractor with providing this service. According to Component A officials, funding was not provided because of agency-wide funding issues. Component A officials also said that there was a requirement that the alternate site be part of the DHS data center consolidation project. However, the CIO's office has not provided guidance to the components on construction of alternate sites or a schedule of when the consolidated data centers would be available.

⁵ The Department of Homeland Security, Office Inspector General, has redacted the names of specific components from this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552 (b)(2). A review under the Freedom of Information Act will be conducted upon request.

A third Component A facility with four servers did not have a fully operational disaster recovery site. Recovery plans for these critical IT systems identify a remote Component A facility as the alternate site. However, the identified site does not have all the equipment necessary to act as a fully operational disaster recovery site. An extended disruption in the operation of the IT systems at this facility could hinder the performance of some of Component A's mission essential functions.

Component B

A Component B facility with 32 servers did not have an identified alternate site. While this deficiency has been reported to Component B's management, additional funds had not been provided to acquire a disaster recovery site. This facility is located in a geographic region subject to natural disasters. An inadequate disaster recovery capability could hinder Component B's ability to respond effectively to a demand for assistance in the disaster area.

Furthermore, Component B was responsible for two additional facilities that did not have fully operational disaster recovery sites. The larger of these two Component B facilities, with 200 servers, has a signed lease for an alternate disaster recovery site. However, as of April 2004, the implementation plan for this capability had not been deployed or tested. Additionally, the alternate site for the smaller facility, with 41 servers, is another Component B facility. Again, the disaster recovery plans to implement this capability have not been prepared or tested. A significant disruption in the operation of the IT systems at either facility may hinder the performance of mission essential activities, (b) [redacted]
(b) [redacted]

Component C

We, and our independent verification and validation (IV&V) contractor, observed a disaster recovery test for a facility that contained six mainframes and 180 servers. While Component C was able to restore operations, the recovery time for one critical system did not meet the requirement established in the business impact analysis. The minimal recovery time for this system was exceeded due to the time required to transfer backup tapes from Component C's tape storage facility to the recovery site, combined with the time required to restore the system with the tape backups.

Component C was testing a data replication methodology as a potential solution to this deficiency.

Other deficiencies existed that were related to Component C's use of a commercial facility for recovery purposes. Specifically, Component C personnel were pre-positioned at the recovery site before the test began. Pre-positioning personnel ensured that all critical staff were available for the scheduled test and enabled Component C to meet recovery goals by reducing the recovery time by several hours that would have been needed for travel. Component C informed us that it could not perform an unscheduled recovery test due to the need to schedule the test times with the vendor.

Additionally, Component C's contract for this commercial facility only allowed a set period of time for testing. When this scheduled time elapsed, Component C had not completed all activities associated with removing data from storage devices. Component C then relied on the vendor to complete the data removal process. Component C has taken steps to ensure that, in future tests, the data removal process will be completed before Component C leaves the facility.

Potential effects associated with an extended outage of the IT systems running at the Component C facility include a disruption to the enforcement of laws governing (b) [redacted] (b) [redacted] and excessive overtime. A disruption in processing capability also could impact non-Component C users of these systems, including the private sector, (b) [redacted] (b) [redacted], as well as other DHS components and federal agencies.

Component D

Component D was responsible for three facilities, containing a total of 123 servers, which did not have an identified disaster recovery site. Component D is working to identify an alternate site and to provide the required resources for an adequate backup and recovery capability for its critical systems. Failure of identified IT equipment at these facilities could inhibit the ability of DHS

(b) _____

(b) [redacted]

employees to perform mission essential functions or to communicate within DHS and with outside stakeholders.

Component D also used a contractor-owned facility that contained 97 servers. Not all of the IT systems operating at this facility had backup and recovery capabilities. During OIG fieldwork, Component D took action to acquire and equip a separate DHS location to provide for a fully operational disaster recovery capability. Access to DHS internet and intranet sites could be restricted if a service disruption occurred at this facility before a fully functioning alternate site is implemented.

Component E

A Component E facility contained 97 servers and two mainframes. Component E tested its disaster recovery plans in conjunction with the government-wide COOP exercise, *Forward Challenge 04*, in May 2004. As a result of this effort, Component E identified a shortfall of IT assets and has been acquiring the necessary equipment to remedy the deficiency. Additionally, Component E has undertaken efforts to acquire a recovery site that is at a more appropriate distance from its operating facility. An inadequate disaster recovery capability may delay or prevent Component E from carrying out its mission functions efficiently or effectively during a major catastrophe.

Component F

Component F is responsible for a facility with 94 servers and is in the process of acquiring the use of a more distant disaster recovery site. Component F had tested recovery plans and noted a need for higher speed communication lines. Following our IV&V contractor's review of this component's disaster recovery training, testing, and exercise documentation, the contractor rated this facility a *Center of Excellence*. The contractor cited the identification and training of emergency personnel, the disaster planning processes, the performance of risk assessments, and the inclusion of state and local responders in a recovery exercise as the basis for this rating.

A second Component F facility with 50 servers did not have a fully operational disaster recovery site. Recovery plans for these critical IT systems identify remote Component F facilities as the alternate sites. However, the identified sites do not have all the equipment

necessary to act as a fully operational disaster recovery sites. An extended disruption in the operation of the IT systems at this facility could hinder the performance of some of Component F's mission essential functions.

Component G

Component G was responsible for two facilities that did not have fully operational disaster recovery sites. Component G plans to use an unfurnished DHS facility as an alternate site for one facility with 14 servers. However, Component G is in the process of preparing and equipping this DHS facility to serve as a fully operational recovery site.

A second Component G facility was contractor-owned, contained 35 servers, and did not have a fully operational alternate site. Not all the functions of this second Component G facility could be restored at the Component G contractor's disaster recovery site. Additionally, Component G had not identified the funds necessary to equip this recovery site adequately, or to task the contractor with providing all the necessary recovery services. The two Component G facilities contain IT systems, which cannot experience a significant disruption in their operation without hindering the performance of some of Component G's mission essential functions.

Component H

Component H was responsible for one facility with 14 servers that did not have a fully operational disaster recovery site. Component H plans on using a remote facility as a recovery site. Currently, the identified site does not have all the equipment necessary to act as a fully operational disaster recovery site. However, Component H is augmenting this site as funds and resources become available. An extended disruption in the operation of the IT systems at Component H's facility could hinder the performance of some of its mission essential functions.

Component I

Component I was responsible for one facility with 45 servers that did not have a fully operational disaster recovery site. Component I plans on using a remote facility as a recovery site. Currently, the identified site does not have all the equipment necessary to act as a

fully operational disaster recovery site. Component I may be able to function for an extended period of time without the administrative IT systems operating at its facility.

Component J

Component J, responsible for a facility with 19 servers, had performed a successful COOP exercise in July 2004 but identified the need for additional data storage and connectivity improvements. Some of the identified improvements, however, will not be implemented until the component relocates to a new facility in the third quarter of fiscal year 2005.

Disaster Recovery Documentation Needs Improvement

We reviewed disaster recovery related planning documents, in particular, the components’ COOP and contingency plans. A significant number of the planning documentation did not contain current or required information. In particular, the components had not finalized 13 of the 31 (42%) planning documents reviewed, and 25 of the 31 (81%) documents had deficiencies. The results of the documentation review are summarized below in Table 1, *Summary of Disaster Recovery Planning Documents Reviewed*.

Table 1: Summary of Disaster Recovery Planning Documents Reviewed

	Number Reviewed	Number in Draft	Number That Comply With FPC 65 or NIST SP 800-34	Number With Identified Deficiencies
COOP Plans	10	3 (30%)	7 (70%)	4 (40%)
Contingency Plans	21	10 (48%)	13 (62%)	21 (100%)
Total	31	13 (42%)	20 (65%)	25 (81%)

See Appendix D, *DHS Disaster Recovery Planning Documents Reviewed*, for details.

Adequate COOP and contingency plans provide DHS management with some assurance that mission essential functions will be performed despite a disruption in operations. Without adequate disaster recovery documentation, DHS may not be able to restore critical IT systems supporting those functions within required time frames.

We reviewed the 10 COOP plans to determine if they complied with FPC 65. Six of the 10 (60%) COOP plans were not accurate or current or did not contain required information, such as an inventory of critical IT systems. Adequate COOP plans are required to ensure the continued performance of mission essential functions under all circumstances.

Additionally, we reviewed contingency plans for IT systems to determine if they complied with NIST SP 800-34. Just over half of the contingency plans complied with the NIST format and contained the recommended information. We reviewed the contingency plans to determine whether they could serve as a template to execute the recovery strategy for the IT systems in the event of a disruption. Deficiencies existed in all the contingency plans reviewed. For example, while NIST SP 800-34 recommends that the business impact analysis be performed and included in the contingency plan, only one such analysis was performed. Without performing this analysis, there is no guarantee that the recovery strategy employed will ensure that critical systems are restored within required time frames.

DHS Does Not Have an Enterprise-Wide Disaster Recovery Program

DHS has not implemented a DHS-wide program to coordinate and upgrade the disaster recovery capability for its critical IT systems. The disaster recovery program was inadequate at each of the facilities reviewed. Further, the DHS components responsible for those facilities are trying to resolve identified IT disaster recovery deficiencies at the component level even though several of the components have not been able to identify the funds or resources necessary to implement an adequate disaster recovery capability. Disaster recovery weaknesses at all DHS components may not be resolved fully until implementation of an enterprise-wide disaster recovery solution.

The CIO had taken some actions to implement a DHS-wide disaster recovery solution prior to the start of this audit. First, the

DHS Disaster Recovery Planning Needs Improvement

CIO formed the Enterprise Infrastructure Board (EIB) and chartered this board with several infrastructure consolidation initiatives to meet the vision of “One Network, One Infrastructure, One DHS.” The EIB produced a draft in October 2003, *Roadmap to One DHS IT Infrastructure Version 1*. According to this document, DHS will integrate, consolidate, and transform diverse infrastructures into one to create and implement a world class IT infrastructure.

Second, the CIO created the DHS Data Center Consolidation (DCC) project to support the DHS IT infrastructure roadmap. The DCC project planned to provide DHS with two geographically-separate data centers where all existing and future computing infrastructure could be located. The two planned data centers were to provide mirror computing (duplicate computing resources) at each center. This plan would ensure that each center would have full operational capability to support all data processing requirements should the other data center fail. Further, the CIO created the DCC working group to survey DHS’ legacy data centers and request information concerning the size of the data centers and disaster recovery capability. The group’s efforts have been incorporated into DHS’ Infrastructure Transformation Office, which is responsible for achieving the agency-wide goal of one infrastructure.

The Infrastructure Transformation Office has developed a program to transition the IT infrastructures of the individual DHS components into an integrated infrastructure. However, this program has not made the consolidation of DHS’ data centers a high priority. As a result, the CIO has not informed the components when a consolidated data center will be available to perform disaster recovery activities.

Recommendations

We recommend that the DHS CIO:

Recommendation 1: Allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems.

Recommendation 2: Require that disaster recovery capabilities are included in the planning and implementation of new systems.

Recommendation 3: Require that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards.

Management Comments and Our Evaluation

We obtained written comments on a draft of this report from DHS. We have incorporated the comments where appropriate and included a copy of the comments in their entirety as Appendix B. DHS generally agreed with each of our recommendations. Below is a summary of DHS' response to each recommendation and our assessment of the response.

Recommendation 1: Allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems.

The DHS Office of the CIO agrees that additional funding could be applied toward the development of an enterprise-wide disaster recovery program for mission critical systems. The report recognizes the efforts of the DHS Infrastructure Transformation Office, which is analyzing DHS data centers to determine the most effective and efficient way to provide these capabilities. This effort will also incorporate a DHS-wide disaster recovery program.

We accept DHS' response to incorporate a DHS-wide disaster recovery program as part of the Infrastructure Transformation Office's efforts. However, DHS has not identified the additional funds that might be applied to this effort or how soon a suitable DHS disaster recovery alternate facility may be acquired.

Recommendation 2: Require that disaster recovery capabilities are included in the planning and implementation of new systems.

The DHS Office of the CIO concurs. In its comments, the DHS Office of CIO states that the report correctly concludes that there is a lack of readiness amongst DHS operational elements concerning IT disaster recovery capability and protocols. Many of the geographically dispersed IT assets of DHS are inappropriately housed in urban office buildings and depend entirely on public telecommunications infrastructure for interconnectivity. DHS states that it plans to address these issues through its Infrastructure Transformation Office effort.

We accept DHS' response to address these issues through the Infrastructure Transformation Office.

Recommendation 3: Require that disaster recovery related documentation for mission critical systems be completed and conform to current government standards.

The DHS Office of the CIO does not dispute the importance of having disaster recovery related documentation for mission critical systems developed to consistent standards.

We accept DHS' response as to the importance of having adequate and standardized disaster recovery related documentation.

Purpose, Scope, and Methodology

The overall objective of this audit was to evaluate the effectiveness of DHS' acquisition and management of disaster recovery alternate sites for the general support systems comprising its network backbone. Nineteen DHS facilities were within the audit scope. These facilities are the responsibility of:

- Border and Transportation Security
 - Customs and Border Protection
 - Federal Law Enforcement Training Center
 - Transportation Security Administration
- Emergency Preparedness and Response
 - Federal Emergency Management Agency
- Immigration and Customs Enforcement
- Information Analysis and Infrastructure Protection
- DHS Management Directorate
- The Office of Inspector General
- The United States Coast Guard
- The United States Secret Service

We reviewed DHS communications diagrams, facility surveys, prior audit reports, disaster recovery related documentation, such as COOP and contingency plans, and wiring diagrams. Auditors performed on-site inspections, interviewed key personnel, and contracted for an IV&V assessment of disaster recovery plans and tests. OIG auditors and IV&V contractors also observed disaster recovery tests. Fieldwork was performed at Washington, DC area facilities, as well as at other facilities around the country.

We provided the CIO and DHS components with briefings and presentations concerning the results of fieldwork and the information summarized in this report. Additionally, we provided comments on other deficiencies observed at the operating facilities, including:

- Servers not backed-up.
- Servers not connected to an uninterruptible power supply.
- Servers and telecommunications equipment without adequate environmental and electrical controls.
- Server rooms lacking adequate fire detection or suppression systems.
- Inadequate storage of backup tapes.
- Lack of redundancy in the telecommunications system.
- Wiring closets in unsecured locations or without adequate environmental controls.
- Disaster recovery test not monitored by government personnel.

We conducted this audit between November 2003 and December 2004 at various DHS directorate and organizational elements in the Washington, DC metropolitan area and around the country. We performed its work according to generally accepted government auditing standards and pursuant to the Inspector General Act of 1978, as amended.


We appreciate the efforts by DHS management and staff to provide the information and access necessary to accomplish this audit. The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits (202) 254-4100 and Roger Dressler, Director, Information Systems and Architectures (202) 254-5441. Major OIG contributors to the audit are identified in Appendix E.



**Homeland
Security**

DATE: 25 April 2005

MEMORANDUM FOR: Richard L. Skinner, Acting Inspector General

FROM: 
RDML Ronald Hewitt,
Acting Deputy Chief Information Officer

SUBJECT: Response by the DHS Office of the CIO to the Draft Audit Report -
*Disaster Recovery Planning for DHS Information Systems Needs
Improvement* (OIG-IT-04-003)

General Comments

The DHS Office of the Chief Information officer (CIO) thanks you for the opportunity to comment on the subject report. The results provided in the draft report comprise both observations and recommendations. The observations are valuable to our program improvement efforts and the recommendations are generally consistent with our plans.

OIG Recommendations Recommendations

The report offered three recommendations:

- 1 - DHS CIO should "allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems."
- 2 - DHS CIO should "require that disaster recovery capabilities are included in the planning and implementation of new systems" should also be supported to comply with U.S. policy "to have in place a comprehensive and effective program to ensure continuity of essential federal functions under all circumstances."
- 3 - DHS CIO should "require that disaster recovery related documentation for mission critical systems be completed and conform to current government standards."

CIO Response

The DHS Office of the CIO makes the following responses to each recommendation:

Appendix B
Management's Response

Response by the DHS Office of the CIO to the Draft Audit Report - *Disaster Recovery Planning for DHS Information Systems Needs Improvement* (OIG-IT-04-003)

Page 2 of 3

Regarding, Recommendation #1 - DHS CIO should "allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems."

The DHS Office of the CIO agrees that additional funding could be applied toward the development of an enterprise-wide disaster recovery program for mission critical systems. The report recognizes the efforts of our Infrastructure Transformation Office, which is analyzing DHS data centers to determine the most effective and efficient way to provide these capabilities. This effort will also incorporate a DHS-wide disaster recovery program.

Regarding, Recommendation #2 – DHS CIO should "require that disaster recovery capabilities are included in the planning and implementation of new systems" should also be supported to comply with U.S. policy "to have in place a comprehensive and effective program to ensure continuity of essential federal functions under all circumstances".

The DHS Office of the CIO concurs. The report correctly concludes that there is a lack of readiness amongst DHS operational elements concerning IT disaster recovery capability and protocols. Many of the geographically dispersed IT assets of DHS are inappropriately housed in urban office buildings and depend entirely on public telecommunications infrastructure for interconnectivity. We plan to address these issues through our Infrastructure Transformation Office effort.

Regarding Recommendation #3 - DHS CIO should "require that disaster recovery related documentation for mission critical systems be completed and conform to current government standards"

The DHS Office of the CIO does not dispute the importance of having disaster recovery related documentation for mission critical systems developed to consistent standards.

In closing, we would like to present the comments of three component CIO organizations:

Comments from US CIS

Citizenship and Immigration Services systems not supported by the ICE shared services agreement were omitted from this report. Additionally, USICS Service Center sites located in California, Texas, Nebraska, Vermont, and the National Benefits Center in Missouri were not included in this study. CIS will concur that the systems under the shared services agreement with ICE are implicitly included in the analysis of ICE's capabilities. However, we believe the OIG should conduct a separate study or interview CIS regarding disaster recovery needs and direction.

Comments from US Secret Service

The report specifically addresses the lack of a Business Impact Analysis (BIA) in our 800-34 Continuity Plans. We have no disagreement with this finding. The Secret Service Information Assurance (IA) Staff has a template for completing full contingency planning documents, to include BIAs. Completing full contingency plans for each system requires resources not currently available to the IA staff, so we are unable to provide a realistic estimated completion date for this activity at this time.

Appendix B
Management's Response

Response by the DHS Office of the CIO to the Draft Audit Report - *Disaster Recovery Planning for DHS Information Systems Needs Improvement* (OIG-IT-04-003)

Page 3 of 3

Comments from EP&R (FEMA)

EP&R appreciates the information provided by the Inspector General and recognizes the importance of maintaining effective disaster recovery plans and security controls. We will ensure that the actions recommended by the Auditor are implemented, to the extent that resources permit. We will continue to monitor this area to make improvements where needed. We appreciate the support provided by the Inspector General. We are addressing the findings that pertain to EP&R/FEMA.

(b)
(b)

(b)

- FEMA officials responsible for Continuity of Operations (COOP) and IT Contingency Plans cited in the draft audit report have been advised of the auditors comments and are asked to update their plans to address the findings and recommendations.

With the support of DHS Senior management, the DHS Office of the CIO is committed to addressing deficiencies called out in the report with either implementation, planning or design activities as dictated by priorities, funding, timing and resources.

Additional questions regarding this response may be directed to Trisha Christian in my office at (202) 205-1403.

cc: Steve J. Pecinovsky, DHS Liaison
cc: Susan Richmond, USM

Recovery Site Status for Selected DHS Facilities

Facility	Component Responsible	Facility Servers/ Mainframes	Recovery Site	Comments
1	A	103/1	No Identified Recovery Site	Relying on DHS-wide initiatives to resolve deficiencies.
2	A	125/8	No Identified Recovery Site	Relying on DHS-wide initiatives to resolve deficiencies.
3	A	4/0	Not Fully Operational	Purchasing necessary IT assets.
4	B	41/0	Not Fully Operational	Implementing necessary recovery strategies.
5	B	200/0	Not Fully Operational	Implementing necessary recovery strategies.
6	B	32/0	No Identified Recovery Site	Needs to fund additional capabilities.
7	C	180/6	Operational	Cannot restore a critical system in the required time frame.
8	D	97/0	Not Fully Operational	Implementing identified recovery capabilities.
9	D	86/0	No Identified Recovery Site	Developing recovery strategies.
10	D	27/0	No Identified Recovery Site	Developing recovery strategies.
11	D	10/0	No Identified Recovery Site	Developing recovery strategies.

Recovery Site Status for Selected DHS Facilities (Continued)

Facility	Component Responsible	Facility Servers/ Mainframes	Recovery Site Status	Comments
12	E	97/2	Operational	Implementing a recovery site that is at a more acceptable distance from the primary facility.
13	F	50/0	Not Fully Operational	Needs to purchase additional IT assets.
14	F	94/0	Operational	Implementing a recovery site that is at a more acceptable distance from the primary facility.
15	G	35/0	Not Fully Operational	Needs to fund additional capabilities.
16	G	14/0	Not Fully Operational	Implementing necessary recovery strategies.
17	H	14/0	Not Fully Operational	Needs to purchase additional IT assets.
18	I	45/0	Not Fully Operational	Relying on DHS-wide initiatives to resolve deficiencies.
19	J	19/0	Operational	Additional capabilities under consideration for implementation following relocation of primary facility.

Continuity of Operations Documents

Component	Document Title	Draft / Final	FPC 65 Compliance	Comments
B	Component B Continuity of Operations (COOP) Plan 1	Final	Yes	No deficiencies identified.
C	*Component C COOP Plan 1 ⁷	Final	No	On site IV&V revealed that the COOP plan contained inaccurate information.
C	*Component C COOP Plan 2	Final	No	Did not contain line of succession information.
D	Component D COOP Plan 1	Draft	Yes	No deficiencies identified.
E	Component E COOP Plan 1	Final	Yes	Minor comments, for example: Vital records and databases not described in sufficient detail.
F	Component F COOP Plan 1	Final	Yes	This COOP plan does not appear to be a final product. The plan does not provide the inventory of mission critical systems and data necessary to conduct essential operations.
F	*Component F COOP Plan 2	Final	Yes	No deficiencies identified.
F	*Component F COOP Plan 3	Final	Yes	This document is a divisional level checklist that was designed to supplement the Component F COOP Plan 2.

⁷ The OIG's IV&V contractor reviewed documents that are denoted with an asterisk (*).

Appendix D
Disaster Recovery Planning Documents Reviewed

Continuity of Operations Documents (Continued)

Component	Document Title	Draft / Final	FPC 65 Compliance	Comments
I	*Component I COOP Plan 1	Draft	No	Does not identify essential functions
J	Component J COOP Plan 1	Draft	Yes	No deficiencies identified.

Contingency Plan Documents

Component	Document Title	Draft/ Final	NIST SP 800-34 Compliance	Comments
A	Component A Contingency Plan 1	Draft	No	Does not contain plan activation.
E	Component E Contingency Plan 1	Draft	No	No Business Impact Analysis was provided.
E	Component E Contingency Plan 2	Draft	No	No Business Impact Analysis was provided
F	Component F Contingency Plan 1	Final	Yes	Does not include recommended appendices (e.g., vendor contact list, service level agreements, equipment and specifications).
F	Component F Contingency Plan 2	Draft	Yes	Does not include recommended appendices (e.g., Emergency Management, Occupant Evacuation and Continuity of Operations plans).
F	Component F Contingency Plan 3	Final	Yes	Contingency Plan Manager not identified.
F	Component F Contingency Plan 4	Final	Yes	Order of succession not included.
F	Component F Contingency Plan 5	Draft	Yes	Order of succession not included.
F	Component F Contingency Plan 6	Draft	Yes	Order of succession not included.

Contingency Plan Documents (Continued)

Component	Document Title	Draft/ Final	NIST SP 800-34 Compliance	Comments
F	Component F Contingency Plan 7	Draft	Yes	Does not include recommended appendices (e.g., Business Impact Analysis, Occupant Evacuation Plan, Emergency Management Plan).
F	Component F Contingency Plan 8	Draft	Yes	Does not include recommended appendices (e.g., Business Impact Analysis, Occupant Evacuation Plan, and Emergency Management Plan).
F	Component F Contingency Plan 9	Final	Yes	Does not include recommended appendices (e.g., Business Impact Analysis, Occupant Evacuation Plan, and Emergency Management Plan).
F	Component F Contingency Plan 10	Final	No	There is no designated alternate site.
F	Component F Contingency Plan 11	Final	Yes	Does not include recommended appendices (e.g., Business Impact Analysis, Emergency Management Plan, and Occupant Emergency Plan).

Contingency Plan Documents (Continued)

Component	Document Title	Draft/ Final	NIST SP 800-34 Compliance	Comments
F	Component F Contingency Plan 12	Final	No	This may not be a final document as some appendices have sections labeled 'To Be Determined' (e.g., Appendix C-08C).
G	*Component G Contingency Plan 1 ⁸	Draft	Yes	Tape backup procedures were not defined.
G	*Component G Contingency Plan 2	Draft	Yes	Alternate site was not designated.
I	*Component I Contingency Plan 1	Final	No	The plan is only designed for local situations that do not require the use of an alternate facility.
J	Component J Contingency Plan 1	Final.	No	Order of succession not included.
J	Component J Contingency Plan 2	Final	No	Does not contain plan activation.
J	Component J Contingency Plan 3	Final	No	Does not contain plan activation.

⁸ The OIG's IV&V contractor reviewed documents that are denoted with an asterisk (*').

Information Systems and Architectures Division

Roger Dressler, Director
Kevin Burke, Audit Manager
Karen Nelson, Auditor
Domingo Alvarez, Auditor
Scott Sammons, Auditor
Tim Walton, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Under Secretary, Management
DHS GAO/OIG Liaison Officer
DHS Chief Information Security Officer
DHS Office of Security
DHS Public Affairs
CIO Audit Liaison
Director, Compliance and Oversight Program, OCIO

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations
Committees

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.