Department of Homeland Security
Office of Inspector General

DHS' Progress in Disaster Recovery Planning for Information Systems

OIG-09-60

April 2009

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

April 16, 2009

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 as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of DHS' disaster recovery planning for information systems. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and reviews of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust 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.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Table of Contents/Abbreviations

Abbreviations

CIO	Chief Information Officer
CBP	United States Customs and Border Protection
DC1	DHS Data Center in Mississippi
DC2	DHS Data Center in Virginia
DHS	Department of Homeland Security
DHS 4300A Handbook	DHS 4300A Sensitive Systems Handbook
FEMA	Federal Emergency Management Agency
FIPS Pub	Federal Information Processing Standards Publication
FY	Fiscal Year
ICE	United States Immigration and Customs Enforcement
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SSC	Stennis Space Center
SP	Special Publication
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

Executive Summary

In May 2005, we reported on deficiencies in the Department of Homeland Security's disaster recovery planning for information systems. We recommended that the department allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems, require that disaster recovery capabilities be included in the implementation of new systems, and ensure that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards.

Generally, the department has made progress in establishing an enterprise-wide disaster recovery program. Specifically, the department has allocated funds for this program since fiscal year 2005, and by August 2008 had established two new data centers. Further, the department now includes contingency planning as part of the system authorization process and it has issued guidance to ensure that contingency planning documentation conforms to government standards.

While the department has strengthened its disaster recovery planning, more work is needed. For example, the two new data centers need interconnecting circuits and redundant hardware to establish an active-active processing capability. Additionally, not all critical departmental information systems have an alternate processing site. Further, disaster recovery guidance does not conform fully to government standards. Finally, risk assessments of the data centers are outdated.

We are recommending that the Chief Information Officer implement the necessary circuits and redundant resources at the new data centers; ensure that critical departmental information systems have complete contingency planning documentation; and conform departmental contingency planning guidance to government standards. Additionally, the department should reassess data center risks whenever significant changes to the system configuration have been made. The department's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The Department of Homeland Security (DHS) relies on a variety of critical information technology (IT) systems and technologies to support its wide-ranging missions. DHS' IT systems also allow employees to communicate internally and for the American public to communicate with the department. Following a service disruption or disaster, DHS must be able to recover its IT systems quickly and effectively in order to continue performing these mission essential functions.

In May 2005, we reported on deficiencies in DHS' ability to restore its IT systems.[1] Specifically, we reported that DHS' IT disaster recovery sites were not prepared to prevent service disruptions from potentially hindering the department's ability to perform mission essential functions. Further, we reported that the inability to restore DHS' critical IT systems following a disaster could have negative effects on the performance of mission essential functions. We concluded that these potential effects on DHS' mission include a disruption in passenger screening operations, delays in processing grants in response to a disaster, and delays in the flow of goods across United States borders.

In the May 2005 report, we recommended that the DHS Chief Information Officer (CIO):

- Allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems,
- Require disaster recovery capabilities to be included in the planning and implementation of new systems, and
- Require that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards.

In April 2006, DHS issued action plans to address these recommendations.[2] Specifically, the CIO would:

- Establish and maintain two operational data centers with an "active-active" processing capability. Using the active-active approach, each data center will be able to serve as a backup for each other,

[1] *Disaster Recovery Planning for DHS Information Systems Needs Improvement*, OIG-05-22, May 2005.
[2] *Compliance Follow-up to Audit Report – Disaster Recovery Planning for DHS Information Systems Needs Improvement,* OIG-05-22, April 6, 2006.

- Close 16 existing data centers and move the processing into these two new data centers. DHS IT staff would use the active-active processing capability of these two data centers to ensure each mission critical system has a complete disaster recovery capability, and
- Require a completed and tested IT contingency plan prior to authorizing a system to operate.

Additionally, in the first quarter of Fiscal Year (FY) 2006, the CIO provided DHS components with guidance for the development of contingency plans. This guidance, in the form of a template, will ensure that departmental IT contingency planning documentation conformed to government standards.

Results of Audit

DHS Has Made Progress in Establishing a Disaster Recovery Program, but Improvements Are Needed

DHS has taken steps to correct disaster recovery deficiencies identified in our May 2005 report by allocating funds and establishing two new data centers. However, additional work is needed to create the planned active-active processing capability. Specifically, additional telecommunications circuits, redundant equipment, and sufficient computer room floor space are necessary to ensure that these two data centers can be backup sites for each other.

Progress in Funding and Establishing Data Centers

DHS addressed our recommendation to allocate the funds needed to implement an enterprise-wide disaster recovery program for mission critical systems. Specifically, DHS has allocated funding and established two new data centers as part of its strategy to mitigate disaster recovery deficiencies. Funds for the first data center, called DC1, have been appropriated every year since FY 2005. Additionally, in FY 2008, DHS awarded a multi-year contract not to exceed $391 million to Computer Sciences Corporation to manage DC1.

DC1, also called the National Center for Critical Information Processing and Storage, is a government owned facility at the John C. Stennis Space Center (SSC) in Mississippi. DHS components that have moved systems to DC1 include United States Customs and Border Protection (CBP), United States Immigration and Customs Enforcement (ICE), National Protection and Programs Directorate, and DHS' Management Directorate.

In FY 2008 DHS awarded a multi-year contract not to exceed $820 million to Electronic Data Systems to operate the second data center, called DC2. DC2 is a contractor owned and operated facility in Clarksville, VA. While construction of DC2 continues, the Transportation Security Administration (TSA) and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) office have started transferring IT assets to this facility.

Lack of Connectivity between Data Centers Hinders Recovery Capabilities

DHS has not established the necessary connectivity to ensure that DC1 and DC2 can provide backup capabilities for each other. Specifically, the necessary telecommunications equipment and circuits are not in place to transmit data from one site to the other for backup purposes. Without the necessary connectivity between the two data centers, DHS might not be able to backup and restore mission critical systems within users' required time frames.

Redundant Equipment

DHS has not installed redundant hardware and software at DC1 and DC2 for use in recovering from a systems outage. For example, while resources for Management Directorate systems are installed and operating at DC1, duplicate resources are not installed at DC2. Specifically, DHS has eliminated its Internet gateways from locations in Missouri and Georgia and consolidated them into one gateway at DC1. However, DHS has not installed redundant equipment at DC2 for the Internet gateway. As a result, if DC1 is not accessible, some DHS users may not have access to the Internet.

The need for redundant equipment at DC2 is especially critical due to the single points of failure that exist at DC1. For example, the electrical power for DC1 comes from one sub-station and is routed through one switch room. Similarly, the telecommunications circuits for DC1 come from one building at SSC and are routed through one telecommunications closet. These power and telecommunications single points of failure increase the risk that DHS systems at DC1 may not be accessible following an outage. According to CIO staff, DHS is in the process of procuring the necessary circuits.

Insufficient Computer Room Space

The amount of usable computer room space at DC1 is not sufficient to handle the projected workload. Specifically, DHS plans to migrate processing from 11 data centers to DC1.[3] While DHS has already moved processing from 5 of these data centers to DC1, migrating 4 additional data centers will exceed the available

[3] See Appendix C: DHS Data Centers Migration Schedule to DC1 and DC2.

computer room floor space at DC1 by 2,096 square feet.[4] See Table 1.

Table 1: DC1 Computer Room Space Allocation

	Computer Room Space (Square Feet)	Secure Storage Computer Room Space (Square Feet)	Total Computer Room Space (Square Feet)
Space already in use at DC1	11,738	816	12,554
Migration of United States Coast Guard (USCG) data center from Kearneysville, WV	12,000*	320*	12,320
Migration of Federal Emergency Management Agency (FEMA) data center from Denton, TX	1,120*	520*	1,640
Migration of United States Secret Service (USSS) data center from Washington DC	12,600*	1,110*	13,710
Migration of TSA data center from Annapolis, MD	4,500*	0*	4,500
Total required computer room space at DC1	41,958	2,766	44,724
Total available computer room space at DC1	38,521	4,107	42,628
Total known excess/(shortfall) in computer room space at DC1	**(3,437)**	**1,341**	**(2,096)**

*Data center computer room floor space in FY 2004.

Additionally, migration of processing from the remaining 2 data centers as well as the installation of redundant equipment to provide the active-active processing with DC2 would further increase the shortfall of computer room floor space at DC1. DC1 and DC2 can not be active-active data centers if there is insufficient computer room floor space to house the redundant equipment needed to support disaster recovery operations.

[4] DHS has on-going asset discovery efforts to update the 2004 floor space requirements. Similar discovery efforts, where undertaken, have revealed less floor space usage than the 2004 data call indicated.

According to Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*:

> "Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system."

Additionally, according to *DHS 4300A Sensitive Systems Handbook* (DHS 4300A Handbook):

> "Care must be taken to ensure systems are designed with no single point of failure."

Recommendations

We recommend that the DHS CIO:

Recommendation 1: Provide the necessary resources to ensure that DC1 and DC2 have the connectivity, equipment, and computer room floor space to act as alternate processing sites for each other.

Recommendation 2: Provide redundancy to eliminate reported power and telecommunications single points of failure at DC1.

Management Comments and OIG Analysis

The DHS Acting CIO concurred with both recommendations. These recommendations will be considered resolved but open pending verification of all planned actions.

Contingency Planning for Critical DHS Systems Needs Improvement

DHS requires that disaster recovery capabilities be included in the planning and implementation of new systems. Specifically, before authorizing information systems to operate, DHS requires a completed and tested IT contingency plan for system authorization. However, in FY 2006 and FY 2007 DHS authorized the operation of critical systems that did not have an alternate processing site and critical systems that had incomplete contingency planning documents.[5]

We reviewed contingency planning information for systems whose security categorization in each security objective of confidentiality, integrity, and availability was categorized as high.[6] During FY 2006 and FY 2007, DHS authorized 27 critical systems to operate, of which 8 (30%) did not have an identified alternate processing site. See Table 2.

Table 2: Critical DHS Information Systems without an Identified Alternate Processing Site

DHS Component	System Name	Alternate Site (Y/N)
Management Directorate	DHS Interactive	N
Management Directorate	Sunflower Asset Management System	N
Management Directorate	DHS Online	N
Management Directorate	Stennis Data Center LAN	N
USCG	Shipboard Command and Control System	N
US-VISIT	Automated Biometric Identification System	N
TSA	TSANet	N
TSA	TSA Operating Platform	N

Additionally, only 4 of the 27 critical systems (15%) had contingency plans that had been tested fully. Specifically, 17 (63%) of these systems had only a limited contingency test, such as a table top exercise. Further, the contingency plans for 6 of these systems (22%) had not been tested in the last year. Without a full contingency plan test at an alternate

[5] See Appendix D, *Critical DHS Systems Approved to Operate in FY 2006 and FY 2007.*

[6] Federal Information Processing Standard Publication (FIPS Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides guidance for categorizing information systems based on the three security objectives of confidentiality, integrity, and availability. The security categories are low, moderate, and high. Additionally, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidance for controls based on the security objectives and categories.

processing site, DHS critical systems might not be able to recover in a timely fashion after an outage.

Further, 15 of these 27 critical systems (56%) did not include the required business impact analysis with the contingency plan. A business impact analysis is used to determine contingency requirements such as maximum allowable outage times. For example, if the maximum allowable outage is four hours, a recovery process would need to be designed to resume processing within four hours at an alternate site.

According to DHS 4300A Handbook:

> "When testing is required, IT Contingency Plans shall be tested/exercised annually."

Additionally, according to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, when a system's availability security objective is categorized as high:

> "The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing."

According to NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*:

> "The BIA [Business Impact Analysis] enables the Contingency Planning Coordinator to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities."

Recommendation

We recommend that the DHS CIO:

Recommendation 3: Ensure that business impact assessments are performed, alternate processing sites are identified, and contingency plans tested annually for critical DHS information systems.

Management Comments and OIG Analysis

The DHS Acting CIO concurred with recommendation 3. This recommendation will be considered resolved but open pending verification of all planned actions.

DHS' Guidance for Disaster Recovery Related Documentation Needs Improvement

DHS addressed our previous recommendation to require that disaster recovery-related documentation for mission critical systems be completed and conform to current government standards. Specifically, the CIO provided guidance to DHS components for the preparation of contingency plans. This guidance, the DHS 4300A Handbook Attachment K, *IT Contingency Plan Template*, details the information that is to be included in contingency planning documentation. However, this template is incomplete. Specifically, the template does not include the following information:

- Backup operations plan,
- Written access controls policies and procedures, and
- Preservation of audit information.

The addition of the above items to the template will help ensure DHS components will be able to develop better plans for restoring systems. For example, inclusion of documented access control policies and procedures in the contingency plan reduces the risk of unauthorized disclosure, modification, or destruction of the data residing in the restored systems.

Additionally, DHS contingency planning guidance does not conform fully to government-wide standards. Specifically, according to NIST SP 800-53, if an agency has a system with a high impact for availability, it should have an alternate site. However, DHS has created an exception to this requirement. Specifically, DHS components shall not categorize a system as high impact for availability if it does not have an alternate site. According to DHS 4300A Handbook:

> "If resources for establishing an alternate site are not available or identified, then a system shall not be categorized as high impact for availability."

Contingency planning security controls are based on the potential impact to organizations or individuals should there be a loss of system availability. This potential impact to availability is categorized as low, moderate or high. For example, according to NIST SP 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*:

> "The consequences of disruption of access to information or information systems associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and

personnel within the United States may be severe. Also, anti-terrorism missions are not reliably tolerant of delays. The availability impact level for information systems that ensure the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is high."

Recommendations

We recommend that the DHS CIO:

Recommendation 4: Update the contingency planning template to include all required contingency planning information.

Recommendation 5: Revise the DHS 4300A Handbook to comply with government-wide contingency planning guidance.

Management Comments and OIG Analysis

The DHS Acting CIO concurred with both recommendations. These recommendations will be considered resolved but open pending verification of all planned actions.

DHS Needs to Reassess the Risks Associated with DC1 and DC2

The DHS risk assessments for DC1 and DC2 are out of date and incomplete. Additionally, there are unmitigated threats and vulnerabilities at DC1 and DC2 that may impact their ability to conduct normal operations. DHS should re-assess the risks associated with operating these data centers and establish sufficient controls to mitigate unacceptable weaknesses.

Risk Assessment for DC1

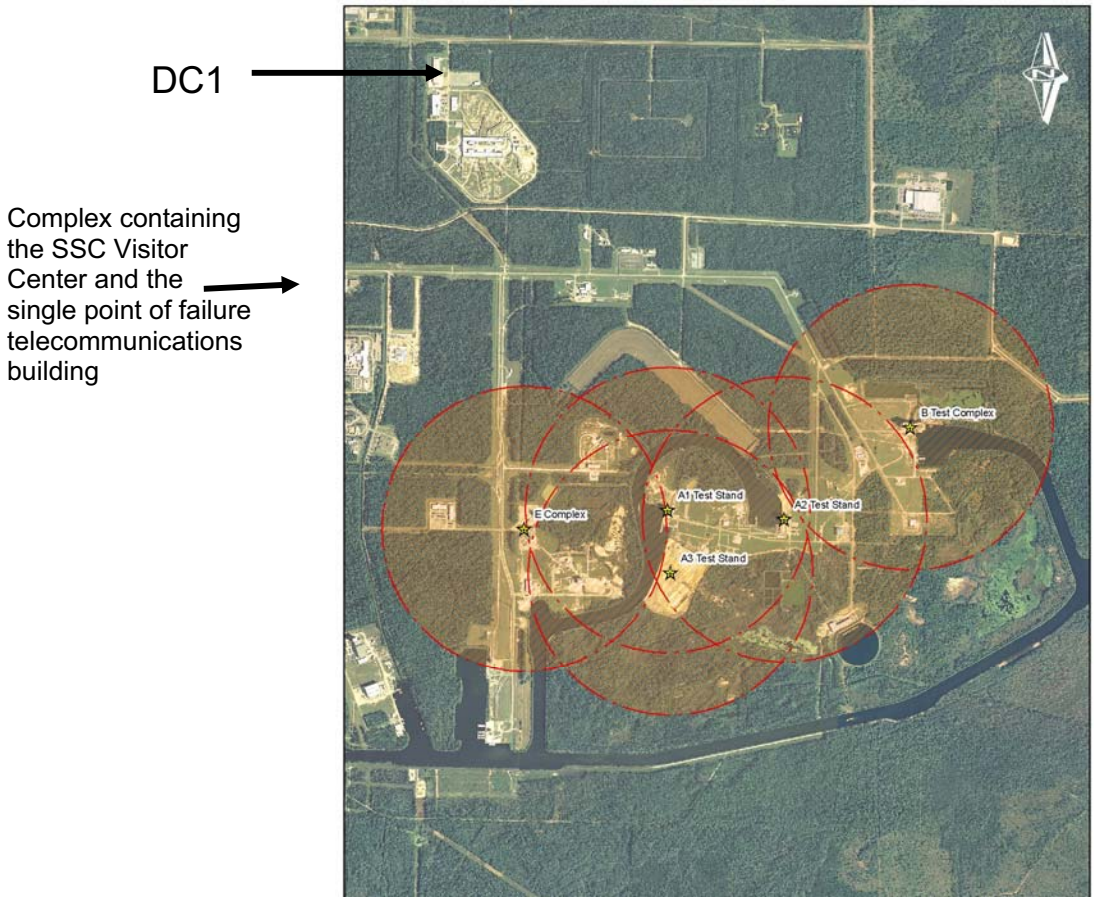
DHS performed a risk assessment on DC1 in July 2006. However, it was not updated when the telecommunications systems were installed. Further, the risk assessment did not include specific threats and vulnerabilities that might place DHS systems at risk. These include:

- Being located within 2 miles of a rocket test facility,
- Being located in a former munitions assembly plant,
- Being located 20 miles from the Gulf Coast, and
- The clearance level of the facilities guards and contractors.

For example, the DC1 risk assessment did not quantify the risk associated with a potential rocket engine test or explosion even though DC1 is located within two miles of a rocket test facility. See Figure 1. Specifically, the assessment did not state if the facility would be accessible in the event of a catastrophic rocket engine test failure. The assessment also did not include the risks associated with acoustical vibrations associated with a normal engine test even though the facility is within a 125,000-acre acoustical buffer zone.

Additionally, the risk assessment did not address environmental contamination. DC1 is in a facility that once was used to construct howitzer shells. Risks associated with working in a former munitions facility, such as lead contamination or unexploded munitions, should be quantified to ensure the safety of staff and their ability to operate the facility.

Figure 1: DC1 is within 2 miles of SSC rocket engine test facilities.



Further, DC1 is located approximately 20 miles from the Gulf Coast, which is vulnerable to a hurricane's damaging winds and floods. However, the risk assessment did not recommend the development of action plans to prepare for potential impacts from hurricanes. These impacts could include the lack of access of operating personnel, flooding, and power failures.

There are also unmitigated vulnerabilities at DC1. For example, the initial risk assessment identified the need for a perimeter fence around DC1. As of December 2008, DHS still had not funded installation of the fence. This perimeter fence will be especially important as StenniSphere, the official SSC Visitor Center, is less than a mile from DC1, and it is accessible by anyone with a valid driver's license or passport.

Risk and Physical Assessments for DC2

The risk assessment for DC2 was performed in April 2008, prior to the final implementation of hardware and telecommunications systems. Additionally, the DC2 physical security assessments did not address the placement of two 25,000 gallon diesel fuel storage tanks within several feet of the building. See Figure 2. The risk assessment should disclose the risk of a storage tank fire either damaging the walls of the facility or restricting safe exit from the building.

Figure 2: Diesel fuel tanks and backup generators adjacent to DC2.

Further, the risk assessment reported that the water-based fire suppression system was considered adequate by the DC2 facility contractor. However, the risk assessment did not cite the potential for damage to equipment from the use of a water-based fire suppression system instead of a clean agent fire extinguishing system, such as the fire suppression system at DC1. For example, the water-based sprinklers are located in both the raised floor computer room and also in the Uninterruptible Power Supply battery room. Accidental discharge of the sprinklers could damage hardware or short out backup batteries.

There are also unmitigated vulnerabilities at DC2. For example, a physical assessment and site survey of DC2 cited the risks associated with maintaining only one guard onsite, rather than the recommended minimum of two onsite guards at all times.

Additionally, a survey for storing sensitive data at DC2 reported that the guards had inadequate clearances for this type of facility.

According to DHS Sensitive Systems Policy Directive 4300A:

> "Components shall conduct and document risk assessments every three years, when high impact weaknesses are identified, or whenever significant changes to the system configuration or to the operational/threat environment have been made, whichever occurs first."

Recommendations

We recommend that the DHS CIO:

Recommendation 6: Re-perform risk assessments at DC1 and DC2 and continue to do so whenever there has been a significant change to the system configuration or the operating environment.

Recommendation 7: Prepare the necessary plans of actions and milestones to mitigate known threats and vulnerabilities associated with DC1 and DC2.

Management Comments and OIG Analysis

The DHS Acting CIO concurred with both recommendations. These recommendations will be considered resolved but open pending verification of all planned actions.

Purpose, Scope, and Methodology

This is the first in a series of reports on DHS disaster recovery planning. Specifically, this audit is a follow-up of our report *Disaster Recovery Planning for DHS Information Systems Needs Improvement (OIG-05-22)*. Each report will address the three recommendations made in the original audit, but will focus on specific DHS components. This report focuses on DHS' Management Directorate and its two new data centers.

The overall objective of this audit was to evaluate the progress DHS has made in the acquisition and management of disaster recovery alternate sites for the general support systems comprising its network backbone. We reviewed DHS policies and procedures, communications diagrams, facility surveys, prior audit reports, contingency planning documentation, and wiring diagrams. Auditors performed on-site inspections and interviewed key personnel.

Our fieldwork was conducted at DHS Management Directorate facilities and organizational elements in the Washington, DC metropolitan area, Stennis Space Center, Mississippi, and Clarksville, Virginia. We conducted this audit between June 2008 and December 2008.

We provided DHS staff with briefings and presentations concerning the results of fieldwork and the information summarized in this report. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We appreciate the efforts by DHS management and staff to provide the information and access necessary to accomplish this audit. The principal Office of Inspector General (OIG) points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits (202) 254-4100 and Sharon Huiswoud, Director, Information Systems (202) 254-5451. Major OIG contributors to the audit are identified in Appendix E.

Appendix B
Management Comments to the Draft Report

Office of the Chief Information Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Margaret H. Graves
Acting Chief Information Officer

MAR 20 2009

SUBJECT: OIG Draft Report, "*DHS' Progress in Disaster Recovery Planning for Information Systems*" – FOR OFFICIAL USE ONLY (FOUO)

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has initiated efforts to address the findings of the Office of the Inspector General Draft Report, *DHS' Progress in Disaster Recovery Planning for Information Systems*, dated January 2009. The response is as follows:

Recommendation 1: Provide the necessary resources to ensure that DC1 and DC2 have the connectivity, equipment, and computer room floor space to act as alternate processing sites for each other.

OCIO Concurs - Both DC1 and DC2 currently have circuits in place to support OneNet, Internet access, and replication between centers. All DHS circuits specific to both DC1 and DC2 are under a detailed review to ensure appropriate installation and funding under the transition from FTS2001 to the Networx contracts. To date, sufficient equipment has been put in place by DHS HQ to accommodate the influx of all DHS Components scheduled to move into the data centers. Additional equipment (network) will be procured as necessary to support future (unscheduled) moves into the data centers. DC1 currently has 43,702 square feet of floor space available, while DC2 has 44,369 square feet of floor space available. Together, there is sufficient available floor space available to meet the needs of the known migration efforts to the data centers. Many of the components are utilizing the consolidation efforts to re-engineer to more current, dense and compact technologies. Overall Component systems are expected to take less space/racks at the DHS data centers than originally planned.

Recommendation 2: Provide redundancy to eliminate reported power and telecommunications single points of failure at DC1.

OCIO Concurs - There is a four phased plan to improve the power distribution to and within DC1. Phase 1 is funded. This phase of the improvement plan provides for redundant power distribution lines to DC1. DC1 currently has circuits with both carrier and geographic diversity to the Stennis Space Center to support OneNet and Internet access. OCIO will continue to collaborate with NASA to plan and develop a secondary data path within the bounds of the Stennis Space Center.

Appendix B
Management Comments to the Draft Report

Recommendation 3: We recommend that the DHS CIO ensure that business impact assessments are performed, alternate processing sites are identified, and contingency plans tested annually for critical DHS information systems.

OCIO Concurs - The DHS Sensitive Systems Policy MD140-1 (formally MD4300) requires that BIA assessments are performed and alternate processing sites be identified if a system requires high availability. As a part of the DHS Certification and Accreditation process, a document reviewer verifies that an alternate processing site has been identified (if appropriate) and a CPT has been performed within the year.

Recommendation 4: Update the contingency planning template to include all required contingency planning information.

OCIO Concurs – The OCIO is reviewing the contingency planning template and will see how to best address this recommendation.

Recommendation 5: Revise the DHS 4300A Handbook to comply with government-wide contingency planning guidance.

OCIO Concurs - The OCIO is reviewing the MD140-1 Handbook to see how best to address this recommendation.

Recommendation 6: Re-perform risk assessments at DC1 and DC2 and continue to do so whenever there has been a significant change to the system configuration or the operating environment.

OCIO Concurs - OCIO will have a new Risk Assessment encompassing all of DC1 and DC2 executed and completed by the end of 2009. System specific risk assessments will be completed for significant changes to the system configuration or operating environment.

Recommendation 7: Prepare the necessary plans of actions and milestones to mitigate known threats and vulnerabilities associated with DC1 and DC2.

OCIO Concurs - OCIO has noted and input the findings of this IG report as Plan of Action and Milestones (POA&Ms) associated to both DC1 and DC2 packages within the Trusted Agent FISMA (TAF) online tool that is monitored and reported on both by the DHS and HQ Chief Information Security Officers.

Appendix C
DHS Data Centers Migration Schedule to DC1 and DC2

Components' Data Center	Migrated to/Plan to Migrate to		Completion Schedule
	DC1	DC2	
CBP			
National Data Center (Springfield, VA)		√	Q4 of FY 2010
Disaster Recovery Facility (Undisclosed)	√		Q2 of FY 2008
ACE (Tyson's Corner, VA)	√		Q3 of FY 2009
DHS Management Directorate			
DHS/CIO (Bluemont, VA)	√		Q2 of FY 2010
DHS Ashburn Data Center (Ashburn, VA)	√		Q2 of FY 2008
DHS HSDN Fair Lakes (Fairfax, VA)		√	Q4 of FY 2008
DHS Stafford Data Center (Garrisonville, VA)	√		Q4 of FY 2007
ICE			
ICE – (Rockville, MD)		√	Q4 of FY 2008
ICE – (Dallas, TX)		√	Q4 of FY 2008
United Sates Citizenship and Immigration Services (USCIS)			
USCIS – DOJ (Rockville, MD)		√	Q1 of FY 2010
USCIS – DOJ (Dallas, TX)		√	Q1 of FY 2010
USCIS – Verizon (Manassas, VA)		√	Q2 of FY 2010
US-VISIT			
US-VISIT (Rockville, MD)		√	Q2 of FY 2011
US-VISIT (Dallas, TX)		√	Q4 of FY 2009
FEMA			
Information Technology Services Center (Bluemont, VA)		√	Q4 of FY 2009
FEMA (Denton, TX)	√		Q2 of FY 2010
TSA			
IBM St. Louis Hosting Center (Hazelwood, MO)		√	Q4 of FY 2008
TSA Headquarters (Arlington, VA)		√	Q1 of FY 2009
Annapolis Junction Data Center (Annapolis, MD)	√		Q2 of FY 2010
Colorado Springs Data Center (Colorado Springs, Co)	√		Q2 of FY 2010
Atlantic City Data Center (Atlantic City, NJ)	√		Q2 of FY 2011
USCG			
Aircraft Repair and Supply Center (Elizabeth City, NJ)		√	Q4 of FY 2010
Coast Guard Finance Center (Chesapeake, VA)		√	Q4 of FY 2010
OIT Data Center (Kearneysville, WV – Continuity Solution)	√		Q3 of FY 2009
USSS			
USSS (H Street, Washington, DC)	√		Q3 of FY 2010
USSS (Undisclosed)		√	Q1 of FY 2011

Appendix D
Critical DHS Systems Approved to Operate in FY 2006 and FY 2007

DHS Component	System Name	Alternate Site (Y/N)	Full Contingency Test (Y/N)	Contingency Test Type	Business Impact Analysis (Y/N)
Management Directorate	DHS Interactive	N	N	Tabletop	N
Management Directorate	Sunflower Asset Management System	N	N	Tabletop	N
Management Directorate	DHS Online	N	N	Tabletop	Y
Management Directorate	Stennis Data Center LAN	N	N	Tabletop	N
CBP	Automated Export System	Y	N	Tabletop	Y
CBP	NDC Mainframe System	Y	N	Tabletop	Y
CBP	Traveler Enforcement Compliance System	Y	N	Tabletop	N
CBP	DHS OneNetwork	Y	N	Tabletop	N
CBP	Automated Targeting System	Y	N	Tabletop	Y
USCG	CGDN Plus Tier 1	Y	N	Three subject	N
USCG	Fleet Logistics System	Y	Y	Scripted Test	Y
USCG	Naval and Electronics Supply Support System	Y	Y	Scripted Test	Y
USCG	Shipboard Command and Control System	N	N	Onsite Hardware Fix	Y
USCG	Automated Mutual Assistance Vessel Rescue System	Y	N	No test in one year	Y
USCG	Maritime Awareness Global Network	Y	N	No test in one year	N
USCG	Marine Information for Safety and Law Enforcement	Y	Y	Scripted Test	Y
USCG	SBU-LAN – Operations Service Center	Y	Y	Full scale test	Y
ICE	Password Issuance and Control System	Y	N	Tabletop	N
ICE	Security Activities Reporting System	Y	N	Tabletop	N
ICE	Student and Exchange Visitor Information System	Y	N	Tabletop	N
FEMA	DHS Texas - GSS	Y	N	Tabletop	N
FEMA	Agile Systems Development	Y	N	Tabletop	N
US-VISIT	Automated Biometric Identification System	N	N	No test in one year.	N
TSA	TSANet	N	N	Tabletop	Y
TSA	TSA Operating Platform	N	N	Tabletop	Y
TSA	TSIS Remote Access to Classified Enclaves	Y	N	Tabletop	N
TSA	Central Information Distribution System	Y	N	Failover	N

Note: These critical systems had security categorizations of "high" in each of the three security objectives of confidentiality, integrity, and availability.

Appendix E
Major Contributors to this Report

Sharon Huiswoud, Director, Department of Homeland Security, Information Technology Audits

Kevin Burke, Audit Manager, Department of Homeland Security, Information Technology Audits

Domingo Alvarez, Senior Auditor, Department of Homeland Security, Information Technology Audits

Matthew Worner, Program Analyst, Department of Homeland Security, Information Technology Audits

Maria Rodriguez, Referencer

Appendix F
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Under Secretary, Management
Assistant Secretary for Office of Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer (CIO), DHS
Chief Privacy Officer
Deputy CIO, DHS
Chief Information Security Officer, DHS
DHS CIO Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, 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 our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.