DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

INFORMATION TECHNOLOGY:

Final Obstacles Removed
To Eliminate Customs Disaster Recovery
Material Weakness

Office of Information Technology

OIG-IT-03-01 September 2003

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, investigative, and special reports prepared by the OIG periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. 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, if any, have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

Clark Kent Ervin
Acting Inspector General

Contents

Appendices

Contents

Abbreviations

ATS	Automated Targeting System
CRF	Commercial Recovery Facility
DHS	Department of Homeland Security
DR	Disaster Recovery
FY	Fiscal Year
GAO	U. S. General Accounting Office
IG	Inspector General
IT	Information Technology
LAN	Local Area Network
NDC	Newington Data Center
OIG	Office of Inspector General
SOP	Standard Operating Procedure

Introduction

Losing the capability to process, retrieve, and protect information electronically maintained can significantly affect an organization's ability to accomplish its mission. Even relatively minor interruptions can result in financial losses, expensive recovery efforts, and inaccurate or incomplete financial and management information. Federal guidelines require agencies to establish contingency plans (i.e., disaster recovery [DR] plans) to ensure continuity of operations during and after the occurrence of a failure in their automated support systems or other unforeseen or unplanned catastrophic event. Plans should be periodically tested to ensure they work as intended. A backup facility can provide the capabilities to replicate and restore critical applications and functions in order to resume operations in the event of a disaster. Untested plans, or plans not tested for a long period of time, may create a false sense of an agency's ability to recover such operations in a timely manner.

The Department of Homeland Security's (DHS) Office of Inspector General (OIG), in conjunction with the Treasury Department's OIG, conducted a review of DR exercises undertaken by the United States Customs Service[1] (Customs) in 2002 and 2003. This audit was initiated as part of the Treasury OIG's Annual Audit Plan for Fiscal Year (FY) 2002 and ongoing efforts to observe DR tests throughout the department. The objectives of this audit were to determine whether Customs implemented prior audit recommendations and evaluate Customs' recovery capability at its Commercial Recovery Facility (CRF). Fieldwork was conducted between June 2002 and June 2003 at Customs' CRF in Sterling Forest, New York.

The results of this report are based solely on our observations of the DR exercises performed in June 2002, September 2002, November 2002, and June 2003. We did not evaluate the security controls implemented in any of the recovered operating environments. By mutual agreement with the Treasury OIG, the DHS OIG is issuing the final report. See Appendix A for a detailed discussion of our purpose, scope, and methodology.

[1] On March 1, 2003, Customs became part of a new agency within DHS and is now know as the Bureau of Customs and Border Protection. However, for this report, we will refer to the bureau simply as Customs.

Results in Brief

Customs has made significant progress in resolving the longstanding material weakness regarding its non-existent disaster recovery capability. Specifically, Customs contracted with a vendor to provide a facility and support services for restoring its computer operations in the event of a disaster. Also, Customs established a detailed process to help ensure the recovery of its computer operations. During its first comprehensive DR exercise at the CRF, Customs successfully restored the majority of its Newington Data Center (NDC) computer operations (i.e., mainframe, local area network [LAN], and UNIX platforms) and established connectivity to selected field offices and trade partners.

However, we identified areas where Customs could better ensure the successful restoration of its computer operations in the event of a disaster. Specifically, we found that the UNIX Recovery Team was not able to initialize the Sol and Hercules Oracle databases that reside on UNIX servers. As a result, one mission-critical application (the Automated Targeting System [ATS] – People) did not become operational during the recovery test. Also, we found that the incorrect configuration of the firewall denied a trade partner access during one of the mainframe connectivity tests. During the DR exercise, Customs used situation reports to track potential problems, issues, or concerns. We found that some of the information recorded in the situation reports was inconsistently documented or incomplete. In addition, documentation and back-up tapes were transported and stored in containers that were not fire-resistant.

We recommend a number of actions that Customs can take to improve its disaster recovery capabilities, including:

- Implementing technology to enable the initialization of the Sol and Hercules Oracle databases within the established recovery timeframe;
- Configuring the mainframe firewall to allow remote access by trade partners;
- Ensuring that disaster recovery operations center team members are provided with specialized training on how to complete situation reports; and,
- Ensuring that back-up tapes are transported in fireproof containers.

In its response to our draft report, Customs management concurred with our findings and recommendations concerning the November 2002 test. Following the test, Customs management developed plans to resolve all issues arising from the November 2002 test. These issues were resolved in a subsequent DR exercise conducted in June 2003. With the success of the June 2003 disaster recovery exercise, the Department of Homeland Security should consider eliminating the material weakness associated with Customs non-existent disaster recovery capability. Customs' response is summarized and evaluated in the body of this report and included, in detail, in Appendix D.

Background

To protect information resources and minimize the risk of unplanned interruptions, an agency should have a process and plan in place to regain critical operations in the event that its automated support systems fail or some other unforeseen potentially catastrophic event occurs. An agency's DR plan should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. Agency plans should be periodically tested to ensure that the necessary procedures to successfully restore operations in an emergency situation are in place.

The Office of Management and Budget's Circular A-130, *Management of Federal Information Resources*, establishes the policy for the management of Federal information resources. Specifically, Appendix III of this circular, *Security of Federal Automated Information Resources*, establishes a minimum set of controls to be included in Federal automated information security programs. In establishing these controls, managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure.

Testing DR plans is an essential part of an effective recovery process. This testing should include determining whether an alternative data processing site will function as intended, and critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, management may be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

The results of DR testing provide an important measure in assessing the feasibility of the DR plan. As such, test results should be reported to senior management so they are aware of the risks associated with continuing operations without an adequate DR plan, and the need to modify the plan or perform additional testing. Because any test of a DR plan is likely to identify weaknesses in the plan, it is important that the plan and related supporting activities, such as training, be reviewed to address these weaknesses.

In addition to its own needs, other federal agencies rely extensively on Customs information technology (IT) to help enforce laws governing the flow of goods and people across American borders, as well as to assess and collect duties, taxes, and fees on imported merchandise. The mainframe, LAN, and UNIX platforms at the NDC support several major applications related to Customs commercial, financial, administrative, and law enforcement activities.

In 1994, the U.S. General Accounting Office (GAO) cited Customs DR capability for its inadequacy. In addition, the Treasury OIG has repeatedly reported this lack of DR capability and suggested that the bureau report this condition as a material weakness. (See Appendix B for a history of the reported deficiencies in Customs continuity of operations capability.) Customs subsequently reported its DR capability as a material weakness in a memorandum, dated May 26, 2000, to the Secretary of the Treasury. This memorandum referenced Section 5(d) of the Inspector General (IG) Act, 5 U.S.C.A. App. 3, which requires the IG to report immediately to the Secretary whenever the IG becomes aware of a particularly serious deficiency in the operations of the Department. Under the same provision of the law, the Secretary was required to transmit a report on Customs' deficiency to Congress within seven calendar days.

In response, Customs created a specialized unit, known as "the disaster recovery operations center team," to address the historical material weakness with its DR capability. In January 2002, Customs hired a vendor to provide recovery services for its computer operations. In the months leading up to the November 2002 DR exercise, the team conducted tests on each component of Customs' comprehensive DR plan. See Appendix C for details of the exercises performed.

Findings

Customs Has Made Significant Progress To Establish A Disaster Recovery Capability

Customs has made significant progress in resolving the longstanding material weakness related to its non-existent DR capability. Customs successfully recovered its NDC computer operations (i.e., mainframe, LAN, and UNIX platforms) and established connectivity to select field offices (Miami, Los Angeles) and trade partners (Clearfreight, Derringer). The field offices and trade partners successfully executed mission-critical application transactions. The mission critical applications included the Automated Commercial System and the Treasury Enforcement Communication System.

During our review, we identified a number of actions taken by Customs, as well as the recovery services vendor, that assisted in establishing Customs' DR capability and will help to minimize service disruptions in the event of a disaster. Specifically, we observed that:

- The CRF had adequate physical controls for off-site recovery. For example, the CRF was located in an unmarked building, in an isolated area. Guards were stationed at the entrance to the CRF campus, as well as the CRF recovery building. Access to the CRF recovery building required photo identification, an access badge, and a personal access code. The personal access code was used for the keypad/locking devices located at all doorways throughout the CRF. In addition, the recovery rooms in the CRF facility contained raised flooring, air conditioning units, fire alarm system, smoke detectors, fire extinguishers, and sprinkler system.

- All participants on the mainframe, LAN, and UNIX recovery teams had access to either an electronic or hard copy of the DR standard operating procedures (SOP). We observed several disaster recovery operations center team members from all three recovery teams using the SOPs during the exercise.

- A computer operations recovery test plan was established for the DR exercise. Specifically, the test plan identified: (1) the testing schedule; (2) staffing, personnel, and logistics; (3) command and control procedures; (4) security procedures; (5) success criteria for each platform; (6) back-up tape procedures; (7) test processes for the mainframe, LAN, and UNIX environments; (8) integrated test processes and goals; and (9) extended goals if primary goals were achieved. In the testing schedule section of the test plan, starting and ending times were established for each task. All completion times were recorded by a designated observer and the results were tracked at the primary command and control center.

- The situation report forms were used to record problems, issues, and concerns encountered during the exercise. Each report was assigned a tracking identification number. The situation reports allowed for the entering of information pertaining to: (1) the platform that encountered the incident; (2) a description of the incident; (3) the date and time of the incident; (4) the priority of the incident (minor problem or a major disruption); and (5) supporting documentation.

- Customs established a logistical process for its personnel and back-up tapes used in the DR exercise. The bureau used ground transportation to ensure that the disaster recovery operations center team and shipment of back-up tapes used for the recovery process arrived at the CRF in a timely manner. Customs also used ground transportation to ensure that team members were transported from the their hotel to the CRF during work-shift rotations. Additionally, security personnel guarded the back-up tapes and recovery documentation throughout the entire exercise.

- The disaster recovery operations center team created a “lessons learned” document after each of the five (four component and one comprehensive) DR exercises performed during 2002. Our review of these documents showed that they were inclusive and identified specific ways Customs could ensure continued improvement of its DR capability. In addition, we observed that the team effectively communicated with the CRF vendor by conducting meetings to exchange management and technical feedback from the exercise. Effective communication with the vendor will assist in further improving Customs’ DR capability.

Although Customs met the primary goals established for the mainframe and network platforms, the primary goals established for the UNIX platform were met only partially. Also, configuration problems were encountered regarding firewall security. Though situation reports were used to track potential problems, issues, or concerns during the DR exercise, we found that some of the information recorded was either inconsistent or incomplete. In addition, back-up tapes used to recreate the computer operations needed further protection.

UNIX Platform Test Goals Were Not Completed

The UNIX Recovery Team was not able to initialize the Sol and Hercules Oracle databases that reside on the UNIX servers. Although, the UNIX recovery team encountered configuration problems with host bus adapters[2] that delayed the initialization of the databases, the team concluded that these databases were too large (approximately three terabytes each) to initialize in the given timeframe. This resulted in one mission-critical application's (ATS – People) not functioning fully.

Mainframe Firewall Was Not Correctly Configured

During connectivity testing, the configuration of the firewall prevented an authorized trade partner access to the production mainframe. To allow the trade partner access, the team had to eliminate the security of the firewall. Once the firewall security was eliminated, the trade partner was successful in accessing the production mainframe, and transactions were executed successfully.

Process For Identifying Recovery Problems Was Inconsistent And Incomplete

Customs used situation reports to track problems, issues, and concerns during the recovery exercise. The reports were forwarded to the command center and the information recorded was used to ensure that problems encountered during this disaster recovery exercise are corrected for future exercises. We found, however, that some of the information recorded in the situation reports was either inconsistent or incomplete. For example, our review of reports relating to the mainframe environment identified instances where the "Situation Description" and "Priority of Situation" sections were left blank. Also, the detail of problems, issues, or concerns identified in the "Situation Description" section varied among the team individuals that were assigned to record the situation reports. For example, in some reports, the "Situation Description" sections were written in detail, while some were general and brief. The lack of sufficient detail could

[2] A host bus adapter is an input/output adapter that connects a host input/output bus to a computer's memory system. A "bus" is defined as a network topology or circuit arrangement in which all devices are attached to a line directly, and all signals pass through each of the devices.

prevent the team from accurately identifying the problem and adequately correcting it. Further, the team members assigned to write the situation reports were not provided specific training on how to assign the priority level for an incident. Although general training was provided for team members assigned to develop situation reports, management agreed that more specific training needs to be provided for recording information in the reports.

Back-up Tapes And Documentation Need Further Protection

Although Customs had security personnel guard the back-up tapes and documentation throughout the exercise, these items were not maintained in fireproof containers. Back-up tapes and recovery documentation are essential to any successful disaster recovery plan. Storing the back-up tapes and recovery documentation in fireproof containers throughout the exercise would provide further protection of these essential items.

Recommendations

OIG recommends that the Commissioner of Customs and Border Protection direct the Chief Information Officer, Customs and Border Protection to:

1. Acquire technology to enable the initialization of the Sol and Hercules Oracle databases within the established recovery timeframe;

2. Configure the mainframe firewall to allow remote access by trade partners;

3. Ensure that specialized training is provided to all disaster recovery operations center team members on how to complete the situation reports; and,

4. Ensure that back-up tapes are transported in fireproof containers.

Management Comments and OIG Evaluation

Management Comments

In its written comments to the draft report, Customs concurred with our recommendations and planned to implement appropriate actions to correct the weaknesses identified. The bureau demonstrated the following actions taken through the results of the June 2003 DR test at the CRF:

- Customs successfully recovered the databases that support the ATS mission-critical application within the established recovery timeframe. Access to ATS via multiple technologies was achieved by the disaster recovery operations center team to ensure its availability to the user community.
- The firewall configuration that had previously denied a trade partner access during one of the mainframe connectivity tests in November 2002 was resolved. All five trade partners were successful in connecting to the CRF through the firewall during the June 2003 test.
- Specialized training on completing situation reports was provided to all technical observers prior to the June 2003 test. The reports were used throughout the June test, and the information recorded in the reports was consistent and complete across all technologies. A LAN was also installed at the CRF to ensure that the technology areas being tested could communicate with the Command and Control Center.

Although Customs management acknowledged that the current practice for the transport and storage of documentation and back-up tapes does not include the use of fire-resistant containers, they took additional steps to minimize the exposure of data during transport. Specifically, (1) multiple backups for each day of activity are transported to the CRF to ensure recoverability; (2) media is shipped in industry standard transport containers; and (3) media is shipped via multiple vehicles.

<u>OIG Evaluation</u>

The OIG agrees that the formal steps Customs management has taken satisfies the intent of the recommendations.

* * * * * *

We would like to extend our appreciation to Customs for the cooperation and courtesies extended to both the DHS and Treasury OIG staffs during the review. If you have any questions, please contact Frank Deffer, Assistant Inspector General for Information Technology, at (202) 254-4100, or Edward G. Coleman,

Purpose, Scope, and Methodology

The overall objectives of this review were to determine whether Customs implemented prior audit recommendations and evaluate the bureau's DR capability at the CRF. These objectives were accomplished by identifying whether Customs had taken corrective actions to remedy previous weaknesses identified by observing four DR exercises at the CRF. The results of this report are based on observations of the DR exercises at the CRF, and our review of related documentation created by the disaster recovery operations center team.

Of the five exercises that were conducted during 2002, we observed two component exercises, as well as the comprehensive restoration of the computer operations. Specifically, during June 2002, we observed the component recovery exercise for the mainframe and LAN platforms. We then observed the component exercise conducted during September 2002, which tested the frame relay connectivity between the CRF and Customs field offices and trade partners. Finally, we observed the comprehensive DR exercise conducted in November 2002. The primary goal of the November exercise was to integrate the previous component testing and validate the test plans and procedures developed to recover the NDC computer operations. We also observed the DR test conducted in June 2003 to ensure corrective actions were taken to address the weaknesses we identified during the November 2002 test.

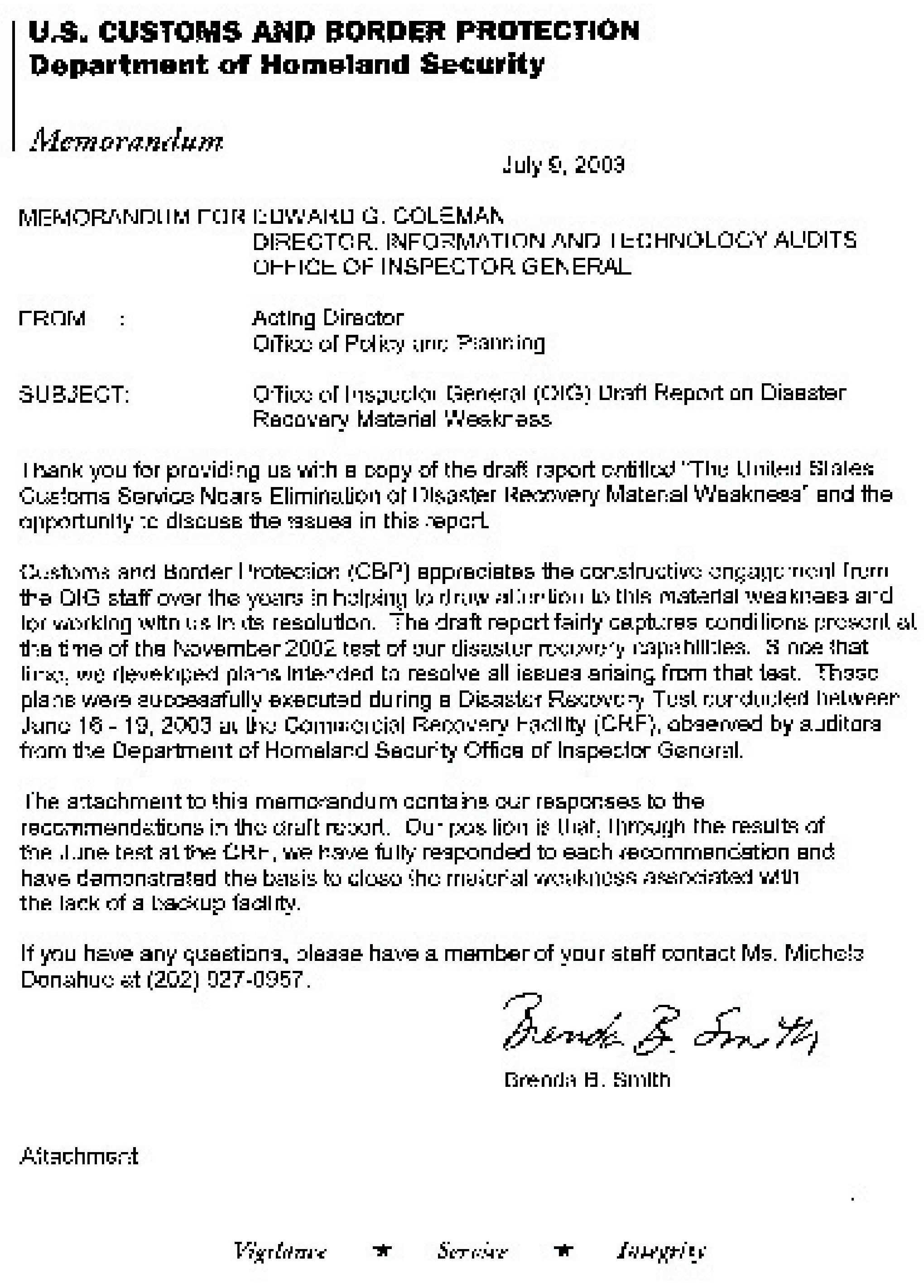
We conducted our audit between June 2002 and June 2003 in accordance with generally accepted government auditing standards. The results of this report are based solely on our observation of the DR exercises involving Customs and its CRF. We did not evaluate the security controls for any of the recovered operating environments.

References To Prior Audit Recommendations

			Report Title
			Financial Management: Customs Controls Over Sensitive Computer Programs and Data Were Weak
	OIG-95-131		U.S. Customs Service's EDP General Controls Continue To Be Weak
	OIG-96-098		Additional Information On Reportable Matters Related to the Audit of the U.S. Customs Service's Fiscal Year 1995 Consolidated Financial Statements
	OIG-97-054		Report on the United States Customs Service's Fiscal Years 1996 and 1995 Consolidated Financial Statements
	OIG-98-050		Report on the United States Customs Service's Fiscal Years 1997 and 1996 Consolidated Financial Statements
	OIG-99-109		Final Report on the U.S. Customs Services Continuity of Operations Capability
			Deficiencies in U.S. Customs Service Automated Systems
	OIG-00-115		Final Report on the U.S. Customs Services Disaster Recovery and Computer Security Programs

DR Exercise Objectives and Results

Date	Objective	Exercise Results
June 11, 2002 to June 14, 2002	Test the plans and procedures developed to recover the mainframe and LAN platforms at the CRF.	Successfully recovered mainframe and LAN platforms.
July 18, 2002 to July 20, 2002	Test the plans and procedures developed to recover the UNIX platform at the CRF.	UNIX platform was recovered except for the Sol and Hercules servers.
September 10, 2002 to September 14, 2002	To test and accept one DS-3 circuit to ensure that the circuit was operational for the 9/21 test. The DS-3 circuits are used for network connectivity and for the relay circuits utilized for communication to the CRF.	The disaster recovery operations center network team successfully tested one DS-3 circuit.
September 20, 2002 to September 21, 2002	Test frame relay connectivity between the CRF and select remote locations (field offices, trade partners).	Remote connectivity was achieved, however the firewall had to be disengaged to allow one trade partner access.



U.S. CUSTOMS AND BORDER PROTECTION
Department of Homeland Security

Memorandum

July 9, 2003

MEMORANDUM FOR EDWARD G. COLEMAN
DIRECTOR, INFORMATION AND TECHNOLOGY AUDITS
OFFICE OF INSPECTOR GENERAL

FROM : Acting Director
Office of Policy and Planning

SUBJECT: Office of Inspector General (OIG) Draft Report on Disaster Recovery Material Weakness

Thank you for providing us with a copy of the draft report entitled "The United States Customs Service Nears Elimination of Disaster Recovery Material Weakness" and the opportunity to discuss the issues in this report.

Customs and Border Protection (CBP) appreciates the constructive engagement from the OIG staff over the years in helping to draw attention to this material weakness and for working with us in its resolution. The draft report fairly captures conditions present at the time of the November 2002 test of our disaster recovery capabilities. Since that time, we developed plans intended to resolve all issues arising from that test. These plans were successfully executed during a Disaster Recovery Test conducted between June 16 - 19, 2003 at the Commercial Recovery Facility (CRF), observed by auditors from the Department of Homeland Security Office of Inspector General.

The attachment to this memorandum contains our responses to the recommendations in the draft report. Our position is that, through the results of the June test at the CRF, we have fully responded to each recommendation and have demonstrated the basis to close the material weakness associated with the lack of a backup facility.

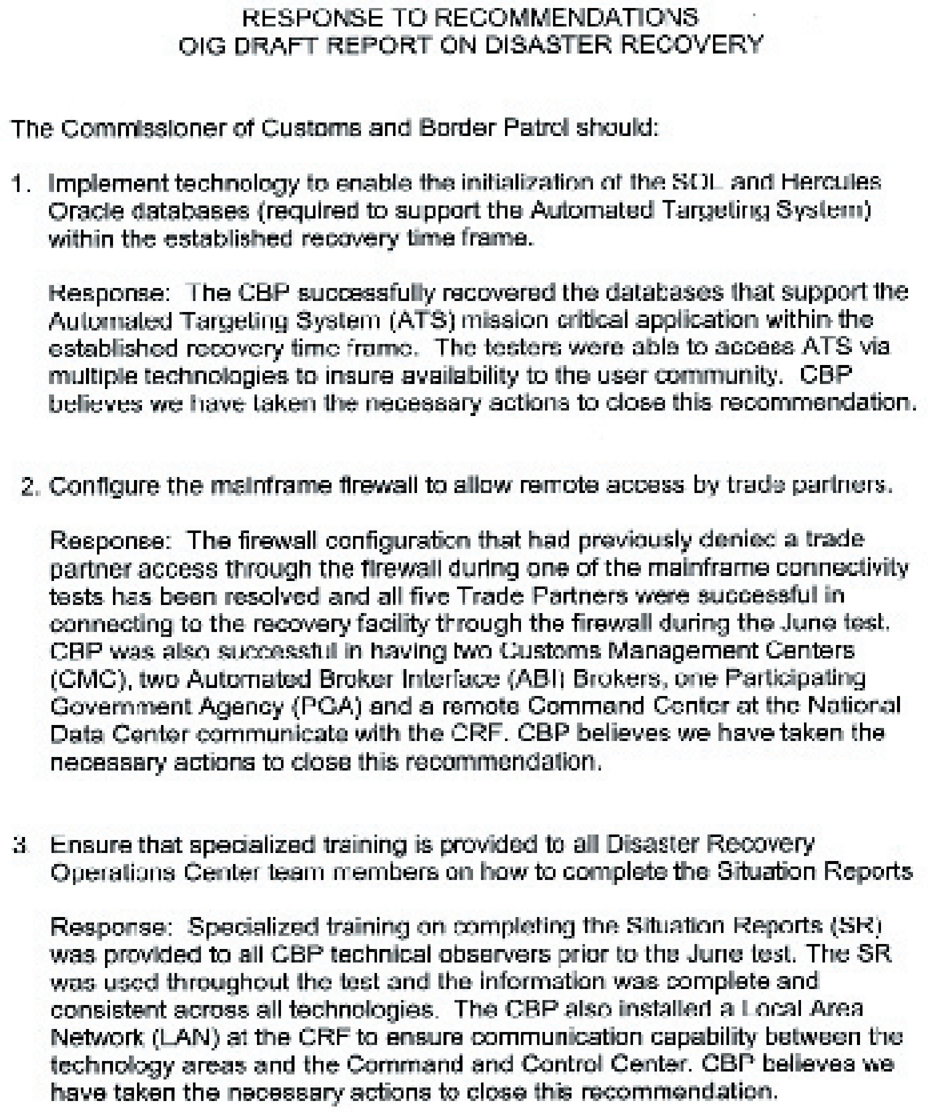
If you have any questions, please have a member of your staff contact Ms. Michele Donahue at (202) 927-0957.

Brenda B. Smith

Brenda B. Smith

Attachment

Vigilance ★ Service ★ Integrity



RESPONSE TO RECOMMENDATIONS
OIG DRAFT REPORT ON DISASTER RECOVERY

The Commissioner of Customs and Border Patrol should:

1. Implement technology to enable the initialization of the SQL and Hercules Oracle databases (required to support the Automated Targeting System) within the established recovery time frame.

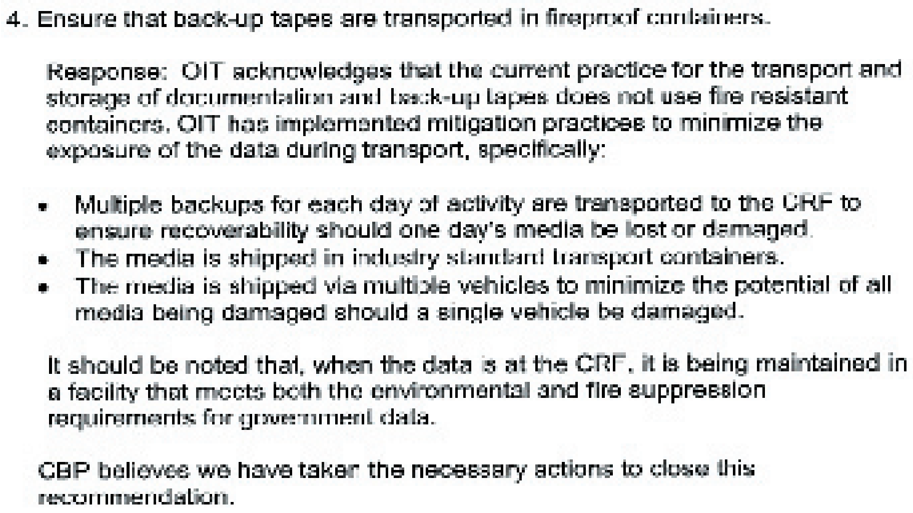
   Response: The CBP successfully recovered the databases that support the Automated Targeting System (ATS) mission critical application within the established recovery time frame. The testers were able to access ATS via multiple technologies to insure availability to the user community. CBP believes we have taken the necessary actions to close this recommendation.

2. Configure the mainframe firewall to allow remote access by trade partners.

   Response: The firewall configuration that had previously denied a trade partner access through the firewall during one of the mainframe connectivity tests has been resolved and all five Trade Partners were successful in connecting to the recovery facility through the firewall during the June test. CBP was also successful in having two Customs Management Centers (CMC), two Automated Broker Interface (ABI) Brokers, one Participating Government Agency (PGA) and a remote Command Center at the National Data Center communicate with the CRF. CBP believes we have taken the necessary actions to close this recommendation.

3. Ensure that specialized training is provided to all Disaster Recovery Operations Center team members on how to complete the Situation Reports

   Response: Specialized training on completing the Situation Reports (SR) was provided to all CBP technical observers prior to the June test. The SR was used throughout the test and the information was complete and consistent across all technologies. The CBP also installed a Local Area Network (LAN) at the CRF to ensure communication capability between the technology areas and the Command and Control Center. CBP believes we have taken the necessary actions to close this recommendation.



4. Ensure that back-up tapes are transported in fireproof containers.

Response: OIT acknowledges that the current practice for the transport and storage of documentation and back-up tapes does not use fire resistant containers. OIT has implemented mitigation practices to minimize the exposure of the data during transport, specifically:

- Multiple backups for each day of activity are transported to the CRF to ensure recoverability should one day's media be lost or damaged.
- The media is shipped in industry standard transport containers.
- The media is shipped via multiple vehicles to minimize the potential of all media being damaged should a single vehicle be damaged.

It should be noted that, when the data is at the CRF, it is being maintained in a facility that meets both the environmental and fire suppression requirements for government data.

CBP believes we have taken the necessary actions to close this recommendation.

Major Contributors

DHS OIG – Information Security Audit Division

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Anthony C. Nicholson, Auditor
Sharell Matthews, Referencer

Treasury OIG – Office of IT Audits

Joseph A. Maranto, IT Audit Manager
Richard G. Kernozek, IT Audit

Report Distribution

Department of Homeland Security

Deputy Secretary
Chief of Staff
DHS OIG Liaison
Undersecretary for Border and Transportation Security
Assistant Commissioner, Office of Information Technology
Acting Director, Office of Policy and Planning

Office of Management and Budget

Homeland Bureau Chief
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate

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 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 Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.