# DEPARTMENT OF HOMELAND SECURITY
# Office of Inspector General

# Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport (Redacted)

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

OIG-08-58

May 2008

*Office of Inspector General*

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

Homeland Security

May 28, 2008

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 lessons learned from the U.S. Customs and Border Protection's management of the network outage at Los Angeles International Airport on August 11, 2007. 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. 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.

Richard L. Skinner
Inspector General

# Table of Contents/Abbreviations



## Appendices



## Abbreviations

| | |
|---|---|
| Bradley Terminal | Tom Bradley International Terminal |
| CBP | U.S. Customs and Border Protection |
| CIO | Chief Information Officer |
| DHCP | Dynamic Host Configuration Protocol |
| DHS | Department of Homeland Security |
| IT | Information Technology |
| LAN | Local Area Network |
| LAX | Los Angeles International Airport |
| NOC | Network Operations Center |
| OIG | Office of Inspector General |
| PDT | Pacific Daylight Time |
| SOC | Security Operations Center |
| TECS | Treasury Enforcement Communications System |

# OIG

*Department of Homeland Security*
*Office of Inspector General*

## Executive Summary

We evaluated actions taken by US Customs and Border Protection (CBP) to address the network outage at Los Angeles International Airport (LAX) on August 11, 2007. We also evaluated actions CBP took to prevent a similar outage from occurring again. We performed onsite inspections at the airport, interviewed department staff, and conducted technical tests of workstations involved in the outage. We also reviewed applicable department policies, procedures, and other appropriate documentation.

The August 11, 2007, network outage at LAX prevented CBP from conducting its normal operations for approximately 10 hours and affected more than 17,000 passengers. CBP has taken actions to ensure that a similar outage does not recur at this airport. These actions include updating its network topology and ensuring that backup systems can be deployed quickly.

We are recommending additional actions that CBP could implement to manage network outages more effectively. For example, the CBP Network Operations Center (NOC) could use onsite support staff more effectively to isolate and resolve outages. Additionally and automatic error notification messages should be established. Further, contingency planning documentation for the network at LAX should be updated.

While CBP has taken actions to prevent an outage from recurring at LAX, the conditions that gave rise to the outage may also exist at other ports of entry. We are recommending that CBP determine whether their actions taken at LAX should also be taken at other ports of entry. CBP management concurred with our recommendations.

# Background

On August 11, 2007, the CBP network at LAX experienced an outage that started at approximately 1:00 p.m. Pacific Daylight Time (PDT) and lasted until 11:45 p.m. PDT.[1] At first, CBP staff experienced response time delays with the computer system used to process passengers. Specifically, CBP reported response time during the outage as averaging 2 to 3 minutes when normal CBP computer system response time is under 5 seconds.

Starting at 4:16 p.m. PDT, CBP officers were not able to perform any queries of their remote databases. At that point, CBP was unable to process arriving passengers using remote systems. Further, full deployment of a backup system was delayed until a field technician started assisting with the deployment an hour later.

According to CBP estimates, this outage affected up to 17,000 passengers. Due to the delays in processing passengers, the international arrival areas filled with passengers and the LAX fire marshal restricted the number of people that were allowed in the waiting areas and jet ways. As a result, new arrivals were not allowed to disembark. These passengers sat on approximately 60 planes on the tarmac for several hours. Other operations at LAX, including international departures, were also affected. Additionally, several international flights were diverted to Ontario International Airport, California, approximately 55 miles away.

[1] See Appendix C, *August 11, 2007, LAX Network Outage Timeline*, for details.

# Results of Review

## Actions Taken During the Network Outage

CBP staff and their communications vendor Sprint took various actions to resolve the outage of the CBP network at LAX on August 11, 2007. Specifically, individuals at LAX and remote locations worked together to identify the cause of the outage and to restore processing.

**12:50 p.m. PDT to 2:00 p.m. PDT**

On August 11, 2007, at 12:50 p.m., PDT, CBP staff at LAX first reported a delayed response time when querying the Treasury Enforcement Communications System (TECS).[2] Additionally, CBP's NOC was alerted that they could not access the LAX router. At 1:16 p.m., PDT, the NOC reported the problem with accessing the router to its communications vendor, Sprint. The CBP Help Desk and Duty Officer were notified of the problem.

The NOC instructed the CBP onsite technician at LAX to restart the communications devices leading to the router by turning them off and on. However, restarting these devices did not resolve the problem. CBP reported query response time was now averaging 2 to 3 minutes, approximately 30 times slower than normal. At 1:55 p.m., PDT, Sprint reported to the NOC that its communications lines were active and its routers at LAX responded electronically. Sprint suggested that CBP restart its communications equipment.

**2:00 p.m., PDT to 3:00 p.m., PDT**

The NOC again asked the CBP onsite technician to restart the communications devices and also to verify that there was power to the router. Sprint confirmed that the circuits were not disconnected. The CBP Duty Officer was notified. At 2:48 p.m., the NOC called Sprint and verified that there was power to CBP's communications equipment. The NOC was to call Sprint back when CBP verified that there was power to the Sprint router.

[2] TECS is a CBP mission-critical law enforcement application designed to identify people and businesses suspected of or involved in violation of federal law. TECS is also a communications system permitting message transmittal among DHS law enforcement offices and other national, state, and local law enforcement agencies.

**3:00 p.m., PDT to 4:00 p.m., PDT**

CBP onsite staff confirmed that there was power to the router. The CBP Duty Officer requested a status update. The NOC established a teleconference call with Sprint and the CBP onsite technician. At 3:57 p.m., PDT, the NOC reported to Sprint that there was power to its router and requested that Sprint dispatch a technician to the airport.

**4:00 p.m., PDT to 5:00 p.m., PDT**

The CBP Acting Port Director and the CBP local area network (LAN) field manager for Southern California requested a status update. The last query of the CBP database from LAX was at 4:16 p.m., PDT. The Sprint technician was dispatched to LAX at 4:20 p.m., PDT.

**5:00 p.m., PDT to 6:00 p.m., PDT**

A second CBP onsite technician arrived at LAX and started assisting in terminals 4 and 5. The NOC provided status information on the outage to the CBP Duty Officer and LAX LAN administrator.

**6:00 p.m., PDT to 7:00 p.m., PDT**

A CBP field technician started assisting at the Tom Bradley International Terminal (Bradley Terminal). CBP's Duty Officer set up a conference call on the outage and provided the number to Sprint and the NOC. CBP's LAX Deputy Field Officer, Southern California area manager, deputy area manager, and Office of Field Operations Duty Officer were provided with a status update.

The Sprint technician arrived at the airport and verified that the Sprint equipment was working correctly. Specifically, while the Sprint router had been responding electronically, Sprint was not able to remotely administer the router. When the Sprint technician restarted the router, it restarted in a "busy" state. However, when the Sprint technician disconnected the LAX LAN and then restarted the router, Sprint was able to remotely administer the

router. This confirmed that the problem was with the CBP LAX LAN and not with Sprint equipment.

**7:00 p.m., PDT to 9:00 p.m., PDT**

Sprint remote network support staff joined the conference call and, with the onsite Sprint technician, started assisting CBP in identifying the problem with the CBP LAX LAN. Sprint remote network support instructed the Sprint technician to connect his laptop computer with a modem to the CBP switch. Communicating through the modem, the Sprint remote network support staff evaluated the traffic on the switch with the laptop's HyperTerminal software.[3]

**9:00 p.m., PDT to 11:00 p.m., PDT**

By approximately 9:00 p.m., PDT, all terminals were now processing passengers by accessing the CBP databases except for the Bradley Terminal.

CBP field technicians started activities to isolate the problem. They disconnected a wireless network and a media converter from the network, but this action did not resolve the outage. At the Bradley Terminal, the CBP field technicians continued trouble-shooting by removing and replacing components of a communications device without first turning the power off, a process known as "hot-swapping" components. During this effort, the device burned out, filling the telecommunications closet with smoke. However, the CBP technicians located a decommissioned switch from another section of the airport, restored functionality, and then continued their problem resolution activities.

[3] Hyper Terminal is a program that comes with the Microsoft Windows operating system.
[4]

**11:00 p.m., PDT to 11:45 p.m., PDT**

CBP field technicians disconnected a circuit at the Bradley Terminal containing 12 devices. CBP staff at the Bradley Terminal could then perform database queries. The 12 devices remained disconnected from the LAX LAN and full processing resumed at 11:40 PM PDT.

## Lessons Learned

CBP has taken actions to ensure that the outage on the LAX LAN does not recur, or if it recurs, that the impact will be minimized. However, further actions are necessary to expedite recovery efforts following a network outage.

Specifically, during future events, the CBP NOC should establish conference calls to keep all interested parties informed of the recovery efforts. The NOC also could more effectively use onsite support staff as well as other information sources. Additionally, CBP should provide diagnostic tools, and establish automated messaging to help identify network problems in a timely fashion. Further, CBP should update the LAX LAN contingency plan to provide better guidance during an outage. Finally, CBP's Security Operations Center (SOC) should improve procedures for controlling devices that may be the cause of an outage.

According to Appendix III of the Office of Management and Budget Circular A-130, *Management of Federal Information Systems*:

> "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."
>
> **********
>
> "Normally the Federal mission supported by a major application is critically dependent on the application. Manual processing is generally NOT a viable back-up option. 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. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner."

## Network Operations Center

CBPs NOC manages CBP's wide area network from a central location. However, on August 11, 2007, the NOC could not remotely access the CBP LAN at LAX If a similar outage were to occur in the future, the NOC could take additional steps to keep staff informed, resolve the outage sooner, and identify the source of the outage.

For example, during the outage on August 11, 2007, several people called the NOC to ask about the status of the outage. These callers included the CBP Duty Officer, the local LAN administrator, and CBP Field Operations staff. However, it was the CBP Duty Officer at LAX who initiated a conference call so that all concerned parties could find out the status. In the future, if an outage is not resolved quickly, the NOC should establish a conference call to keep all parties informed of the status of resolution efforts.

Additionally, the CBP NOC could use onsite CBP field support staff more effectively in future outages. For example, the NOC had the onsite CBP field support technician turn the power off, then back on, to various communications devices. However, restarting these devices did not resolve the outage. At that point, the NOC could have instructed the onsite support staff to perform more "'trouble-shooting" activities. Specifically, the NOC could have instructed the onsite field support staff to remove connections and isolate devices in an effort to identify the cause of the outage.

Further, CBP could provide network management tools to assist in identifying and resolving network problems. The NOC could provide similar tools to onsite support staff. Placing network management tools onsite would allow the NOC to use the onsite support staff more effectively when the network is not accessible from a remote location.

## Additional Information Sources

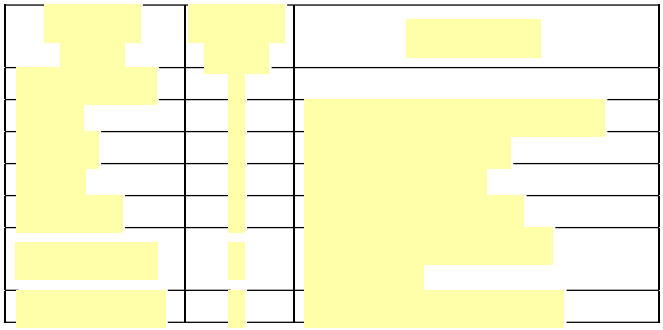
The NOC also could use additional information sources when diagnosing problems with a remote network. For example, during the outage on August 11, 2007, the CBP NOC was concerned that the Sprint circuits to LAX had been disconnected. However, the NOC could have determined that the circuits were active through three different CBP informational sources. Specifically,

- CBP's Automated Operations Division received network traffic information from CBP's LAX LAN;
- The TECS database provided information on whether queries were being received from CBP's LAX LAN; and
- 

Further, the DHCP server may be able to provide the CBP NOC with specific information about the cause of an outage.

## Field Support Procedures

CBP should ensure that field support staff have the training and information necessary to effectively service hardware components. Specifically, these procedures should list which devices are not "hot-swappable." This information would assist onsite support technicians when they are trying to resolve a network outage. For example, a CBP LAX LAN communications device burned out and filled the LAN room with smoke when CBP field technicians erred by removing and replacing components of a communications device without first turning off the device.



**Contingency Planning Documentation**

CBP should ensure that contingency planning documentation is sufficient to guide staff in the event of a general support system failure.

### Security Operations Center Procedures

CBP's SOC should improve procedures for controlling devices that may be the cause of an outage. For example, the CBP SOC's and our evaluations of workstations that may have been involved in the outage were inconclusive. Specifically, the SOC noted that rebooting one of the machines may have eliminated critical information.

Improved SOC procedures for impounding devices and maintaining a chain of custody would assist CBP when performing diagnostics on other workstations that may be involved in a similar outage.

## Recommendations:

We recommend that the CBP Chief Information Officer (CIO) take the following actions for CBP activities at LAX:

**Recommendation #1:** Establish and test procedures to use NOC and onsite field support staff more effectively during a network outage.

**Recommendation #3:** Provide network diagnostic tools for onsite support staff.

**Recommendation #6:** Improve procedures for impounding and maintaining the chain of custody for computers to be evaluated.

## Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the CBP Office of Policy and Planning. We have included a copy of the comments in their entirety at Appendix B.

In the comments, CBP concurred with recommendations one through six. These recommendations will be considered resolved but open pending verification of all planned actions.

## Other CBP Ports of Entry May Experience Similar Outages

According to CBP staff, there is a high risk that a similar outage could occur at other CBP ports of entry. For example, according to an August 2007 briefing CBP provided to the Congress,

[redacted]

CBP has taken various actions to ensure there is no repeat of the August 11, 2007, outage on its LAN at LAX. [redacted]

Further, CBP has updated its systems security plans to include devices operating at LAX. Finally, we have made six recommendations in this report to assist CBP in improving system operations at LAX. CBP should determine whether these improvements should also be applied at other ports of entry.

[redacted]

**System Documentation**

CBP has taken steps to ensure that all known information technology assets are included in the system security plan for the LAX LAN. These include refugee fingerprint processing machines and a network monitoring workstation operated by the Automated Operations Division. These assets may be operating at other ports of entry and may not be included in the appropriate site security plan.

According to DHS 4300 Sensitive Security Handbook, Attachment D – Type Accreditation,

> "To account for unique physical and logical variations at the site level, a description of any differences and the associated risks at each site are documented, and the site-specific documents are incorporated as attachments or appendices to the master C&A package."

## Recommendation:

We recommend that the CBP CIO:

**Recommendation #7:** Determine whether the corrective actions taken at LAX should also be taken at other CBP ports of entry.

## Management Comments and OIG Analysis

In the comments, CBP concurred with recommendation seven. This recommendation will be considered resolved but open pending verification of all planned actions.

## Appendix A
## Purpose, Scope, and Methodology

Our purpose was to determine whether actions taken by CBP to address the August 11, 2007, outage at LAX were sufficient to minimize the effects of a potential future outage. Specifically, we evaluated whether the controls that CBP implemented would assist in identifying the cause of an outage, facilitate deployment of backup systems, and recover from the outage.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer. We mutually agreed to the wording for the Rules of Engagement for the technical testing.[5] We reviewed applicable DHS and CBP policies, procedures, and CBP's responses to our site surveys and technical questionnaires. Prior to performing our onsite review, we used CBP's responses to identify occupied space, server rooms, and telecommunications closets. Our onsite review included a physical review of CBP space and interviews with CBP staff. Our technical review included reviews of workstations that may have been involved in the outage at LAX.[6]

We provided CBP with briefings concerning the results of fieldwork and the information summarized in this report. We conducted this review between August 2007 and March 2008.

We performed our work according to the *Quality Standards for Inspection* of the President's Council on Integrity and Efficiency, 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 review. Our points of contact for this report are Frank Deffer, Assistant Inspector General for Information Technology, (202) 254-4100, and Roger Dressler, Director for Information Systems and Architectures, (202) 254-5441. Major Office of Inspector General (OIG) contributors to the review are identified in Appendix D.

[5] The Rules of Engagement established the boundaries and schedules for the technical evaluations.
[6] Our analysis of three devices that may have been involved in the August 11, 2007 outage was inconclusive.

## Appendix B
## Management Comments to Draft Report

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

May 6, 2008

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Director Will H Houston
Office of Policy and Planning

SUBJECT: U.S. Customs and Border Protection Response to the Office of Inspector General Draft Report entitled "Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport"

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) Draft Report entitled "Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport". Attached is the U.S. Customs and Border Protection (CBP) corrective action plan and comments to the draft report.

The OIG evaluation focused on actions taken by CBP to address the network outage at Los Angeles International Airport (LAX) on August 11, 2007, and evaluated actions taken to prevent a similar outage from occurring again. The report addresses both the strengths and weaknesses in the implementation of security policies and procedures. OIG started the actual on-site evaluation work at approximately the same time that the Office of Information and Technology (OIT) began an initiative to augment the information technology (IT) infrastructure at LAX. This scheduled start allowed the OIG auditors to view and evaluate the LAX system both before and after upgrades were accomplished. Using before and after site visits enabled OIG to give CBP credit for work that has already been completed.

CBP concurred with the seven recommendations contained in the draft report. CBP also noted to OIG staff during the exit conference that there are concerns with implementing some of the recommendations due to the enforcement of other laws or regulations and the Airport Authority's purview over the facility.

With regard to the classification of the draft report, CBP has identified information within the report requiring restricted public access based on a designation of "For Official Use

Only." The information has been annotated in the attached sensitivity comments. A corrective action plan to address the recommendations is also attached.

If you have any questions, please have a member of your staff contact Ms. Janiene Jones at (202) 344-2169.

Attachment

2

**CBP Response and Corrective Action Plans to OIG Draft Report**
**Lessons Learned from the August 11, 2007, Network Outage at LAX**

**Recommendation 1:** Establish and test procedures to use NOC and onsite field support staff more effectively during a network outage.

**Response:** Concur

The CBP Network Operations Center (NOC) has spent extensive man-hours rewriting, refining and reviewing their internal Network Escalation Procedures, Troubleshooting Procedures, and other related documents. These new and/or updated documents are stored on a network share accessible to ALL members of the CBP NOC and will be reviewed and updated periodically to ensure completeness.

CBP will be updating Port Policy 2008-15 to include a testing scheduled to be coordinated with the local staff at a minimum at two times per month. The testing procedure will include Treasury Enforcement Communications System (TECS) Outage, LAN Outage and Power Outage simulation. The updated Port Policy will be completed no later than April 30, 2008.

This is an on-going effort to ensure that CBP NOC troubleshooting procedures and "how-to" documents are up to date and valid, not only for existing team members, but for new team members as we grow. Updates to procedures are ongoing. The update effort started shortly after August 11, 2007, LAX outage. CBP expects to have all the new and/or updated documents accessible to all members of the CBP NOC by May 16, 2008.

**Due Date**: December 31, 2008

[redacted]

**Recommendation 3:** Provide network diagnostic tools for onsite support staff.

**Response:** Concur

CBP is in the process of putting together the requirements to provide the Local Area Network (LAN) Administrators, Field Technology Officers (FTO), etc, with view access to the monitoring tools that are monitoring the infrastructure within their responsibility areas. This is an ongoing effort.

1

Additionally, CBP is in the process of procuring a monitoring and diagnostic tool that will be used by the NOC and onsite support staff. CBP expects to have the above tasks completed by July 25, 2008.

CBP has initiated a strategic enterprise initiative to define and aggregate critical event sources used to monitor systems availability. The aggregation of event data across IT monitoring systems within CBP will enable operators and support technicians to proactively identify and respond to potential system events that could ultimately impact systems availability. Further, the aggregation of event data provides an unprecedented capability within CBP to define business impact by leveraging IT intelligence across multiple IT disciplines within the enterprise. In total, the infusion of a robust Business Service Management capability within CBP will position the organization to proactively identify and resolve issues directly impacting critical business services supporting the mission of CBP.

**Due Date**: September 30, 2009

**Recommendation 6:** Improve procedures for impounding and maintaining the chain of custody for computers to be evaluated.

**Response:** Concur

Since the LAX outage incident, the CBP Security Operation Center (SOC) has created and distributed a CBP-wide custody form and procedure that provides for standardized chain of custody documentation. Two other concerns will be addressed:

- to better socialize security procedures with non-security personnel, so that they are aware of forensic security procedures;
- to include the CBP SOC personnel in the initial stages of a critical outage, such as the event at LAX. By doing so, the CBP SOC can provide guidance if needed during the troubleshooting and forensic process.

Additionally, the CBP SOC will incorporate the chain of custody procedure into the Incident Response training for Information System Security Officers (ISSO) and LAN administrators. The CBP SOC will meet with the CBP NOC to formalize the need for early SOC involvement during significant network incidents.

**Due Date**: September 30, 2008

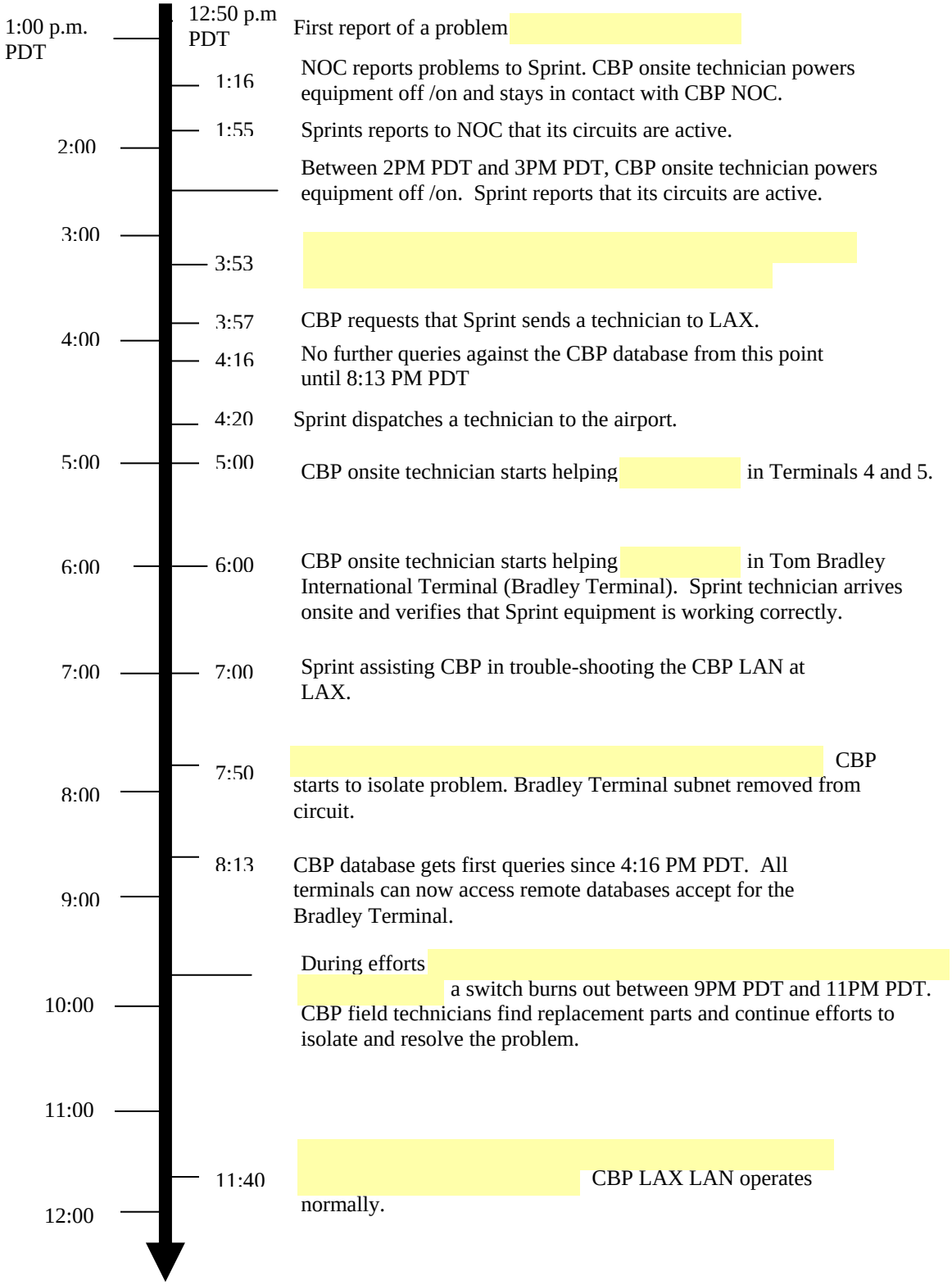
**Recommendation 7:** Determine whether the corrective actions taken at LAX should also be taken at other CBP ports of entry.

**Response:** Concur

As the Systems Availability project implements improvements at additional CBP ports of entry, we will gain additional insights as to the condition of the ports. We can then implement corrective actions that are appropriate to the variable conditions at each location. Ports of entry that will not receive the System Availability upgrades until additional funding is provided are able to utilize the alternative technical solutions, Disaster Recovery capabilities for fail over, as well as the guidance provided by OFO.

**Due Date**: April 30, 2009

**Appendix C**
**August 11, 2007 LAX Network Outage Timeline**



**Appendix D**
**Major Contributors to This Report**

Roger Dressler, 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

Beverly Dale, Senior Auditor, Department of Homeland Security, Information Technology Audits

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

Sammer El-Hage, Program Management Assistant, Department of Homeland Security, Information Technology Audits

Syrita Morgan, Program Management Assistant, Department of Homeland Security, Information Technology Audits

Richard Saunders, Director, Department of Homeland Security, Information Technology Audits

Steve Matthews, Department of Homeland Security
Information Technology Audits

Pamela Williams, Referencer/Senior Auditor, Department of Homeland Security, Information Technology Audits

**Appendix E**
**Report Distribution**

---

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary for Management
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer (CIO)
Chief Privacy Officer
Deputy CIO
Chief Information Security Officer
Commissioner, CBP
Information Systems Security Manager, CBP
CBP Audit Liaison
DHS Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS Program 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) 254-4199, 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.**