Department of Homeland Security
Office of Inspector General

Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project

(Redacted)

OIG-11-42

February 2011

Office of Inspector General

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

Homeland Security

FEB 04 2011

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 the U.S. Customs and Border Protection's management of the System Availability project. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to 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.

Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

Table of Contents/Abbreviations

Appendixes

Abbreviations

ARB	Acquisition Review Board
AP	Acquisition Plan
CBA	Cost-Benefit Analysis
CBP	Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
FY	Fiscal Year
IT	Information Technology
IRB	Investment Review Board
LAN	local area network
LAX	Los Angeles International Airport
LCC	Life Cycle Cost
NAD	Need Analysis Document
OAM	Office of Air and Marine
OBP	Office of Border Patrol
OFO	Office of Field Operations
OIG	Office of Inspector General
OIT	Office of Information and Technology

OMB	Office of Management and Budget
PMG	Project Management Guidebook
SLC	System Life Cycle
WAN	Wide Area Network

Figures

Executive Summary

On August 11, 2007, a network outage occurred at Los Angeles International Airport that interrupted passenger processing by Customs and Border Protection employees for 10 hours. The outage was caused by the failure of a network card on one of the workstations. We reviewed the circumstances surrounding this outage, and in May 2008 reported that there is a high risk of similar outages at other Customs and Border Protection sites. Our objective was to determine whether Customs and Border Protection has effectively designed and implemented a plan to reduce the risk of network outages at other field sites.

Customs and Border Protection has taken steps to improve network capabilities and reduce network downtime at some field sites. Specifically, it initiated the System Availability project by awarding a task order for information technology services. In addition, it worked with business sponsors to develop operational requirements to ensure that systems capabilities are maintained. It also deployed survey teams to conduct site surveys at each field site.

However, Customs and Border Protection did not properly plan and implement the System Availability project. It did not ensure that adequate funding was available, include all at-risk sites, or develop planning documents needed to justify project requirements and cost. Customs and Border Protection ran out of funding and ended the project in February 2010. As a result, hundreds of field sites did not receive the needed upgrades and remain vulnerable to network outages.

We are recommending that the Customs and Border Protection Chief Information Officer reassess the original objectives of the System Availability project and develop a new program according to Department of Homeland Security and Customs and Border Protection policies and procedures to upgrade the network at all remaining at-risk sites.

Background

In August 2007, Customs and Border Protection's (CBP) network at Los Angeles International Airport (LAX) experienced an outage for more than 10 hours that stranded nearly 17,000 passengers. We conducted an audit of the LAX outage, and in May 2008 reported that there was a high risk that a similar outage could occur at other CBP sites.[1] We recommended that CBP's Chief Information Officer (CIO) determine whether the corrective actions taken at LAX should be implemented at other sites. In response, CBP began the System Availability project to improve CBP network capabilities and to provide enhanced levels of network availability, performance, and reliability at the sites.

The System Availability project objectives are to deploy new infrastructure equipment to the local area networks (LAN) at CBP field sites, which includes The project's goals are to improve network capabilities and reduce network downtime. For sites receiving infrastructure upgrades, CBP for the LAN and wide area network (WAN) in order to ensure that no exist.

[1] OIG-08-58, *Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport*, May 2008.

[redacted]

CBP planned to implement the System Availability project at field sites managed by its three business sponsors—Office of Field Operation (OFO), Office of Border Patrol (OBP), and Office of Air and Marine (OAM)—that rely on the network infrastructure for their critical missions. These business sponsors have a total of 646 sites, divided as follows:

- OFO has 333 official ports of entry in the United States, including 15 pre-clearance offices and 21 field offices.

- OBP has 234 facilities nationwide and is the primary federal law enforcement organization responsible for preventing the entry of terrorists and their weapons between official CBP ports of entry. OBP is also responsible for preventing the illicit trafficking of people and contraband between the official ports of entry.

- OAM operates out of 79 locations, which include three domain awareness centers, three training centers, and a maintenance facility. OAM is the world's largest aviation and maritime law enforcement organization. Its mission is to protect the American people and the Nation's critical infrastructure through the coordinated use of integrated air and marine forces to detect, interdict, and prevent acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward or across U.S. borders.

CBP identified the System Availability project as a high priority to quickly begin remediating the conditions at LAX and other priority sites to prevent similar network outages. To improve system availability, CBP issued a sole-source delivery order to an existing CBP modernization contract. The original modernization program includes tasks to reengineer CBP's operational processes and develop new technology infrastructure, computer systems, and software applications to support these processes. CBP also uses this existing contract to develop the high-tech trade system, Automated Commercial Environment.

Results of Audit

Actions Taken to Implement the System Availability Project

CBP initiated the System Availability project to improve network capabilities and eliminate system outages at field sites. Over a 3-year period, it took the following actions to implement the project:

- Awarded a sole-source task order for information technology (IT) services to perform project planning, analysis, site surveys, network design, and project implementation and support.
- Worked with business sponsors to develop operational requirements to ensure that system capabilities are maintained.
- Deployed teams to conduct site surveys and develop site-specific requirements to improve system availability. These surveys identified site-specific design and equipment requirements.
- Developed network designs for each site that provide a detailed, component-level description of the system availability solution to be deployed.
- Accomplished and completed infrastructure upgrades for 67 sites in various phases of the System Availability project.

Despite its actions, CBP did not complete implementation of the System Availability project at all at-risk field sites. The business sponsors provided a list of 207 priority sites to be included in the System Availability project. However, the Project Management Office was able to implement all network upgrades,

In May 2009, CBP reassessed the System Availability project's scope and determined that only the (LAN upgrade) was required and that the were optional. However, after reducing the project's scope, CBP was able to install LAN upgrades at only 67 sites, leaving 140 priority sites vulnerable to potential disruptions. The System Availability project ended in February 2010, when all funding was depleted. Figure 1 displays the number of sites completed by priority and

Figure 1. System Availability Sites Completed

				Total
	43	24	0	67
	43	0	0	43
	6	0	0	6
Total sites where all phases of project were implemented	6	0	0	6

Site surveys and network designs were performed at some of the sites that did not receive a network upgrade. For example, the , Air and Marine site received only a site survey as part of the System Availability project.

CBP sites that did not receive the needed upgrades remain vulnerable to service disruptions such as those at LAX. In addition, the sites may not be able to support critical new applications being deployed across the enterprise. Further, may degrade mission capabilities of existing applications and from being transmitted in a timely manner.

System Availability Project Was Not Properly Planned and Implemented

CBP did not properly plan the System Availability project, nor did it implement the project fully to achieve its stated objectives. Specifically, CBP did not include all the at-risk sites in the scope of the project, obtain adequate funding for full project implementation, or develop planning documents needed to identify requirements and justify funding. As a result, hundreds of sites did not receive the upgrade and remain vulnerable.

Not All At-Risk Sites Were Included in the Project

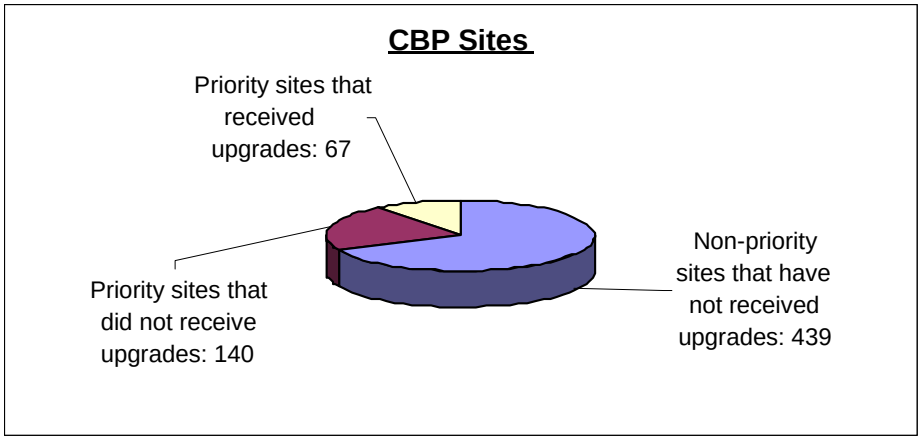
The System Availability project did not include all sites at risk of disruption and failure. Specifically, 579 sites that rely on the network infrastructure, with numerous did not receive the needed upgrades and remain vulnerable to disruptions.

The network assessment study of the CBP LAN revealed many [redacted] at the field sites. CBP business sponsors [redacted] have a total of 646 sites that rely on the network infrastructure for their critical missions. The System Availability project included only 207 sites (32% of the 646 sites). These 207 sites, known as "priority sites," comprise [redacted]

The priority site list featured sites that have high volumes of traffic in passengers and goods entering and leaving the United States. For example, Miami International Airport's daily passenger processing statistics are estimated at 25,000 people for the summer months, and the San Ysidro port of entry estimates 50,000 vehicles and 54,000 pedestrians crossing from Mexico to the United States daily.

Of the 207 priority sites, CBP implemented the required upgrades at 67, leaving 140 sites vulnerable. Further, CBP excluded 439 sites from the project as non-priority locations, bringing the number of sites that did not receive upgrades to 579 (see figure 2). As a result, the excluded sites remain vulnerable to IT interruptions and malfunctions.

Figure 2. CBP Site Status



The System Availability Project Did Not Have Adequate Funding

CBP did not acquire adequate funding to complete the System Availability project. The project received $59 million, which was enough to upgrade 67 sites. The funding shortfall occurred in part because CBP did not follow normal IT budget investment processes for the project. Specifically, CBP did not prepare and submit Office of Management and Budget (OMB) Exhibits 53 and 300 for this project. CBP officials stated that these budget documents were not submitted because this project did not meet applicable dollar thresholds. However, per DHS guidance, the System Availability project is a Level 3 project with a threshold requirement that falls between $50 million and $300 million in life cycle costs (LCCs). As a result, CBP was required to submit an OMB Exhibit 300 to DHS and obtain approval from the DHS Enterprise Architecture Board.

CBP initiated the System Availability project in May 2007, with $5 million in funding from CBP salaries and expenses. Following the LAX outage at the end of fiscal year (FY) 2007, the System Availability project received available year-end funds. FYs 2008 and 2009 year-end funds were also made available. At the end of the project in February 2010, approximately $59 million had been obligated, thus meeting the requirement to prepare the OMB Exhibit 300. When funding ran out in February 2010, CBP terminated the project, leaving 140 priority sites and 439 nonpriority sites without upgrades. Figure 3 identifies the project funding costs by fiscal year.

Figure 3. Project Funding Costs in Millions

Fiscal Year Ended	Total Funds Obligated
2007	$32
2008	$26
2009	$1
Total	$59

Key Planning Documents Were Not Prepared

CBP did not prepare several key planning documents for the System Availability project. Specifically, many of the solution engineering and planning documents required by CBP and DHS

policy were not created. Key planning documents were not completed because the situation was urgent and CBP needed to act quickly to implement upgrades at the field sites.

For example, CBP did not prepare a Project Charter that formally authorizes the existence of a project and authorizes the project manager to apply the organization's resources to the project activities. Per CBP's System Life Cycle Handbook (SLC), Appendix A.3, and Office of Information Technology (OIT) Project Management Guidebook (PMG), Version 2.0, Section 1.2, a project charter is required for all projects. Without a Project Charter, there is no evidence of communication between all affected groups to facilitate coordination of project activities.

Additionally, CBP did not prepare a Need Analysis Document (NAD), which provides the basic information required for the CBP Acquisition Review Board (ARB) to decide on proposed IT projects while they are still in the conceptual stage. A NAD is a brief summary of a project that includes the description, required mission and capabilities, justification, and budget LCC estimate. Per the OIT PMG, Section 1.3, every new CBP project or enhancement to an existing project, regardless of cost or size, must develop a NAD.

CBP also did not prepare a business case to organize the information necessary to justify the project and to make a funding decision in a consistent and structured format, for ARB and Investment Review Board (IRB) reviews. Nor did CBP prepare a cost-benefit analysis (CBA), which includes all resources required to develop and operate the project over its life cycle. As shown in figure 4, per CBP's PMG, Section 1.4.2, the business case and CBA are required for projects with LCCs greater than $20 million.

Figure 4. CBP Documentation Requirements

Project Acquisition/LCC	NAD Required?	Business Case and CBA Required?	CBP Approval Authority Required
Less than $500,000 acquisition or $2 million LCC	YES	NO	OIT, ARB
$500,000 to $5 million acquisition or $2 million to $20 million LCC	YES	NO	CBP, IRB
Greater than $5 million acquisition or $20 million LCC	YES	YES	CBP, IRB

Also, an Acquisition Plan (AP) was not prepared for the System Availability project. An AP forms the basis for the statement of work. Per CBP's SLC, an AP is required for each contracted service that exceeds the $100,000 threshold.

Without these required documents, CBP was not able to develop a good estimate of the project's overall cost. As a result, the project was not completely funded and ultimately was terminated before all priority sites could be upgraded.

Recommendation

We recommend that the CBP Chief Information Officer, in coordination with the Office of Border Patrol, Air & Marine, and Field Operations, reassess the original objectives of the System Availability project and develop a new program in accordance with DHS and CBP policies and procedures to upgrade the network at all remaining at-risk sites.

Management Comments and OIG Analysis

The Assistant Commissioner concurs with our recommendation. We consider the recommendation resolved. CBP is looking forward to working collaboratively with the OIG. Please see Appendix B for DHS' future corrected actions plan

Appendix A
Purpose, Scope, and Methodology

The objective of our review was to determine whether CBP has effectively designed and implemented a plan to reduce the risk of network outages. Specifically, we determined whether (1) CBP has designed a corrective action plan to reduce the risk of network outages at border stations and ports of entry; and (2) CBP has implemented effectively a corrective action plan to reduce the risk of outages at border stations and ports of entry.

We interviewed program executives, program mangers, contracting officers, field deployment and field support technicians, and IT specialists to understand how the Program Office developed and implemented the System Availability project. We reviewed key program documents such as the program management plan, implementation plans, and cost estimates. We also reviewed master spend plans, invoices, and procurement requisitions to determine whether and how cost goals and milestones were met. We reviewed contract delivery orders, contract modifications, and attachments to gain an understanding of contract terms and contractor responsibilities.

Our fieldwork was conducted at CBP sites at headquarters offices and procurement offices in Washington, DC;

We conducted this performance audit between March 2010 and August 2010 pursuant to the *Inspector General Act of 1978*, as amended, and according to 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.

Appendix B
Management Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

November 29, 2010

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

FROM: Assistant Commissioner
Office of Internal Affairs
U.S. Customs and Border Protection

SUBJECT: Response to the Office of Inspector General's Draft Report Entitled, "Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project"

Thank you for providing us with a copy of your draft report entitled "Planning and Funding Issues Hindered U.S. Customs and Border Protection's (CBP's) Implementation of the System Availability Project," and the opportunity to comment on the issues in this report.

The report contains one recommendation directed to CBP. A summary of CBP actions and corrective plan to address the recommendation is provided below:

Recommendation #1: We recommend that the CBP Chief Information Officer reassess the original objectives of the System Availability project and develop a new program in accordance with DHS and CBP policies and procedures to upgrade the network at all remaining at-risk sites.

CBP Response: CBP concurs with the recommendation. CBP will conduct an analysis to determine the scope and resource requirements necessary to address OIG's findings. CBP's targeted completion of the initial analysis is June 30, 2011.

With regard to the sensitivity of the draft report, CBP has identified information within the report requiring restricted public access based on a designation of "For Official Use Only" as it could be used by adversarial parties which seek to cause harm either to the CBP systems or to individuals who would be affected by unauthorized disclosure of the information. Therefore, CBP also includes sensitivity comments.

Please consider CBP's concerns prior to issuing the final report. Thank you for your assistance. If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Ashley Boone, CBP Audit Liaison, at (202) 344-2539.

Attachments

Appendix C
Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Sharell Matthews, IT Audit Manager
Beverly Dale, Team Leader
Domingo Alvarez, Senior IT Auditor
Frederick Shappee, Program Analyst
Pamela Chambliss- Williams Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Respective Under Secretary
DHS Component 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) 254-4100, 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.