

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

CBP Information Technology Management:
Strengths and Challenges
(Redacted)





Homeland
Security

June 29, 2012

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 Office of Information and Technology. 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.

A handwritten signature in black ink, appearing to read "Frank Duff".

Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Executive Summary	1
Background	2
Results of Audit	7
IT Management Capabilities	7
Recommendations	16
Management Comments and OIG Analysis	16
IT Support of Mission Needs	17
Recommendations	27
Management Comments and OIG Analysis	27

Appendices

Appendix A: Purpose, Scope, and Methodology	29
Appendix B: Management Comments to the Draft Report	31
Appendix C: Major Contributors to This Report	36
Appendix D: Report Distribution	37

Abbreviations

ACE	Automated Commercial Environment
ACS	Automated Commercial System
ATS	Automated Targeting System
BPETS	Border Patrol Enforcement Tracking System
CIO	Chief Information Officer
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
E3	The Next Generation of Enforce
EA	enterprise architecture
FY	fiscal year
IT	information technology
ITAR	Information Technology Acquisition Review
MD	Management Directive
OIT	Office of Information and Technology
OMB	Office of Management and Budget
SELC	systems engineering life cycle

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the U.S. Customs and Border Protection's (CBP) information technology management. The objective of our audit was to evaluate the Chief Information Officer's overall information technology management approach, including the extent to which information technology management practices have been put in place and the current information technology environment supports mission needs. Appendix A describes the audit's scope and methodology.

The Chief Information Officer has implemented a strategic planning process, developed an enterprise architecture, and established a systems engineering life cycle process to guide and manage the agency's information technology environment. Additional progress is needed building the agency's target business architecture and implementing oversight of information technology spending across all programs and activities within the agency, which increases the risk of enterprise alignment challenges.

Challenges remain, however, to ensure that the information technology environment fully supports CBP's mission needs. Specifically, systems availability challenges exist, due in part to aging infrastructure. Also, interoperability and functionality of the technology infrastructure have not been sufficient to support CBP mission activities fully. As a result, CBP employees have created workarounds or employed alternative solutions, which may hinder CBP's ability to accomplish its mission and ensure officer safety.

We are recommending that the Chief Information Officer provide needed resources for enterprise architecture activities, ensure compliance with the information technology acquisition review process, develop a funding strategy for the replacement of outdated infrastructure, and reassess the existing requirements and technology insertion processes to address challenges in the field.

Background

CBP is the frontline border security agency within the Department of Homeland Security (DHS). CBP is charged with the priority mission of keeping terrorists and their weapons out of the United States, while facilitating the flow of legitimate trade and travel. CBP's responsibilities include apprehending individuals attempting to enter the United States illegally; stemming the flow of illegal drugs and other contraband; protecting agricultural and economic interests from harmful pests and diseases; protecting American businesses from theft of their intellectual property; regulating and facilitating international trade; collecting import duties; and enforcing U.S. trade laws. In fiscal year (FY) 2012, CBP's budget was approximately \$12 billion, 20 percent of DHS' overall budget of approximately \$60 billion.

CBP has more than 58,000 employees nationwide and overseas. CBP's workforce includes more than 20,000 Border Patrol agents who protect the borders with Mexico and Canada; more than 20,000 CBP officers who screen passengers and cargo at over 300 ports of entry; nearly 1,000 Air and Marine interdiction agents who prevent people and goods, including weapons, narcotics, and conveyances, from illegal entry by air and water; more than 2,200 CBP agriculture specialists who work to curtail the spread of harmful pests and plant and animal diseases; and nearly 2,500 employees in CBP revenue positions who collect over \$30 billion annually in entry duties and taxes through the enforcement of trade and tariff laws. Additionally, CBP has 8,000 employees providing operational and mission support. Figure 1 shows CBP's organizational structure.

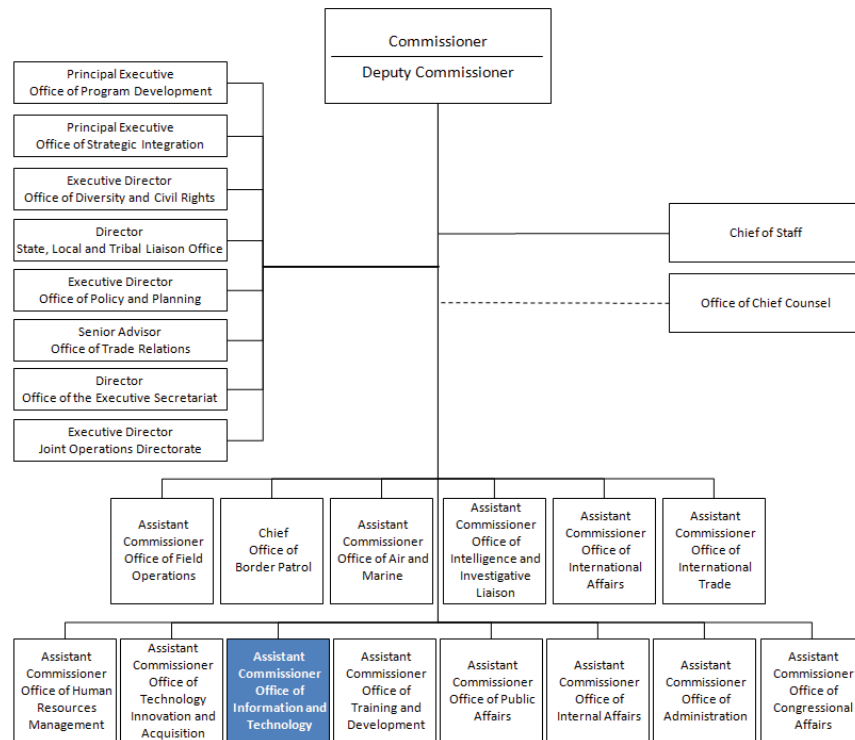


Figure 1. CBP Organizational Structure as of December 2011

CBP’s Office of Information and Technology (OIT) provides information technology (IT) services and products that enable CBP to meet its missions. CBP, with an IT budget of \$1.5 billion in FY 2012, is the largest IT component within DHS, comprising 26 percent of the Department’s \$5.8 billion IT budget. OIT employs 5,399 IT staff—2,231 Federal employees and 3,168 contractors. CBP’s IT operational infrastructure—

- Supports more than 65,000 workstations;
- Processes more than 26 billion database transactions per day;
- Manages the largest DHS data center, with more than 70,000 square feet of floor space; and
- Supports tactical communications infrastructure and equipment for 1,100 tower sites with radio equipment and more than 65,000 mobile and portable radios.

To manage CBP’s critical IT environment, OIT is organized into several offices. Five program offices provide IT expertise in their respective areas. The Passenger Systems Program Office provides application development and continued operational support of traveler and immigration-related systems. The Cargo Systems Program Office is responsible for the development, maintenance, and deployment of systems and interfaces that support CBP, other government agencies, and the trade community regarding the

importation, exportation, and control of merchandise shipments. The Targeting and Analysis Systems Program Office provides solutions that support CBP inspection and enforcement activities to help CBP officers and analysts protect borders. The Border Enforcement and Management Systems Program Office provides concentrated support for border enforcement systems for the Office of Border Patrol, the Office of Field Operations, and the Office of Air and Marine. The Wireless Systems Program Office provides expertise for tactical communications and related wireless efforts.

In addition, there are two enterprise IT management divisions. The Enterprise Data Management and Engineering Division provides enterprise solutions to optimize IT data integrity and accessibility and ensure performance quality, reliability, and 24×7 IT systems availability to support border protection and the facilitation of legitimate trade. The Enterprise Network and Technology Support Division provides operational day-to-day technology support to all CBP field locations, technology training, the enterprise wide area network, security operations, and help desk services.

OIT has two additional support offices. The Field Support Program Office provides onsite customer service and support to CBP's 58,000 employees throughout the United States and overseas to minimize service interruptions in support of the mission. The Laboratories and Scientific Services Office provides forensic and scientific testing in the areas of trade enforcement, weapons of mass destruction, intellectual property rights, and narcotics enforcement. Figure 2 shows the CBP OIT organizational structure.

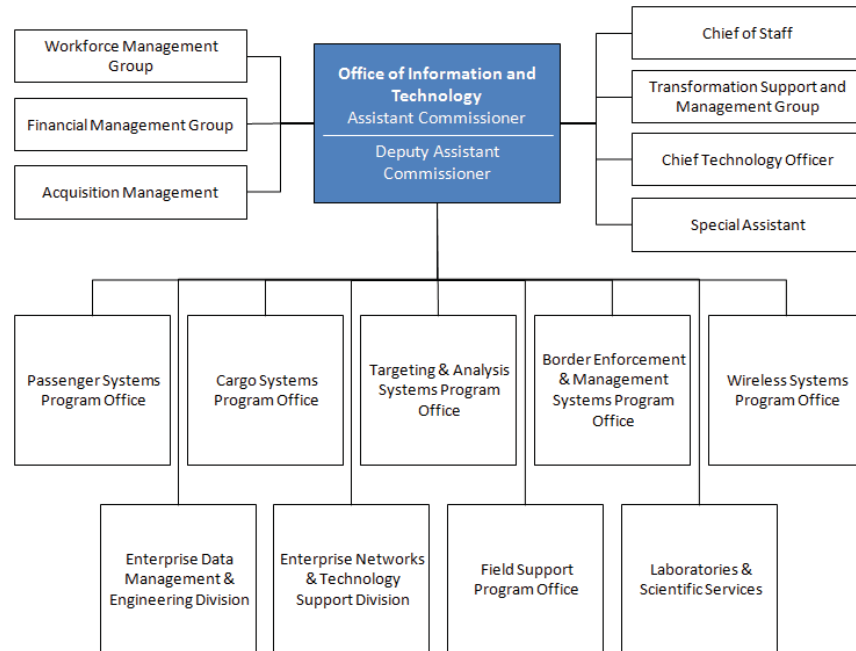


Figure 2. CBP's OIT Organizational Structure as of October 2011

IT systems play a critical role in enabling CBP to accomplish its border security, trade, and travel missions. CBP's OIT supports business processes with the design, development, programming, testing, implementation, training, and maintenance of CBP automated systems. Some of CBP's major commercial and enforcement systems are listed below.

Commercial Systems

- Automated Commercial System (ACS) - ACS is the system CBP uses to track, control, and process all commercial goods imported into the United States.
- Automated Commercial Environment (ACE) - ACE is a commercial trade processing system designed to automate border processing. ACE will eventually replace ACS.

Enforcement Systems

- Automated Targeting System (ATS) - ATS is an Intranet-based enforcement and decision support tool that assists CBP officers and analysts in selecting individuals or cargo that pose a greater risk for violation of U.S. law for additional screening.
- TECS provides computer-based access to enforcement files of common interest, online access to the Federal Bureau of Investigation's National Crime Information Center, and an

interface with the National Law Enforcement Telecommunications System.

- The Next Generation of Enforce (E3) - E3 is a CBP-developed transactional enforcement application that captures all enforcement actions for Border Patrol agents and CBP officers.

The CBP Chief Information Officer (CIO) has undertaken an initiative to transform the way OIT provides IT support to CBP. This transformation initiative will replace CBP's aging IT infrastructure, which is costly to maintain. Most of OIT's budget goes toward operations and maintenance of this outdated infrastructure. At the same time, demand for IT services is growing and becoming more critical for CBP's mission. The CIO estimates that demand for storage and processing capacity is increasing at the rate of 50 percent per year. The CIO must address these issues within the confines of a declining IT budget. The OIT budget has decreased by \$335 million since FY 2009 as funds were reallocated to pay for other CBP shortfalls.

To address these challenges, OIT is leveraging technologies that enable it to operate and deliver customer capabilities more efficiently. To modernize the infrastructure, the CIO is working to replace obsolete technology, migrate to the DHS data center, and move toward private cloud infrastructure where possible.¹ Further, the CIO is transitioning from mainframe to web-based applications and turning off less critical tools.² The CIO also is planning to automate the data center and network management environment by implementing end-to-end monitoring processes that will provide greater visibility into the service levels and costs of services that support CBP's lines of business. Additionally, OIT is transforming its workforce and communications through efforts such as retraining its government employees and contractors and federalizing its workforce.

¹ Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network such as the Internet.

² Mainframe computers are powerful computers used primarily by corporate and government organizations for critical applications. After 2000, most modern mainframes have phased out classic terminal access for end users in favor of web user interfaces.

Results of Audit

IT Management Capabilities

The CIO has taken several actions to support effective stewardship of IT resources. Specifically, the CIO has implemented a strategic planning process to ensure that OIT supports CBP and Department mission and goals. In addition, the CIO has developed an enterprise architecture to ensure that CBP's IT environment is aligned with the Department's architecture, although additional progress is needed in certain key areas. Finally, the CIO has implemented a systems engineering life cycle process to manage IT programs from initiation through retirement. As a result, OIT has critical capabilities in place to help ensure effective IT management and guide future initiatives, such as the CIO's effort to transform the way OIT does business over the next several years.

The CIO, however, does not have full oversight of IT spending across all programs and activities within CBP. Specifically, CBP component offices have submitted IT spending requests that were processed by procurement without going through the IT Acquisition Review (ITAR) process. Component noncompliance with ITAR occurred because component offices and procurement personnel were unfamiliar with the process, and the extended time taken for reviews has been a disincentive. IT acquisitions that do not go through the ITAR process increase the risk of security issues or enterprise alignment challenges.

Strategic Planning

The *Government Performance and Results Act of 1993* holds Federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.³ Additionally, Office of Management and Budget (OMB) Circular A-130, as revised, instructs agency CIOs to create strategic plans that demonstrate how information resources will be used to improve the productivity, efficiency, and effectiveness of government programs.⁴ Finally, DHS Management Directive (MD) 0007.1 requires component CIOs to develop and implement an IT strategic plan that clearly defines how IT supports a component's mission and drives investment decisions, guiding the component toward its goals and priorities.⁵

³ Public Law 103-62, *Government Performance and Results Act of 1993*, August 3, 1993.

⁴ OMB Circular A-130, *Management of Federal Information Resources*.

⁵ DHS, MD 0007.1, *Information Technology Integration and Management*, March 15, 2007.

The CIO has an effective strategic planning process in place to meet Federal requirements and departmental guidance. In 2008, the CIO implemented an IT strategic plan for FY 2009 through FY 2015. In 2011, however, the CIO determined that it was necessary to draft a new plan to address shifts in the OIT budget, emerging technologies, and new departmental direction. The CIO was scheduled to implement a revised plan, the *CBP OIT Strategic Implementation Plan FY 2012-2016*, in March 2012. The draft plan identifies five broad goals, listed in table 1, for achieving OIT’s mission over the next 4 years.

Table 1. OIT Strategic Goals

OIT Strategic Goals				
Goal 1 Modernize and Transform the Infrastructure	Goal 2 Streamline and Automate the Data Center and Network Management Environment	Goal 3 Transform and Shape the Workforce and Communications	Goal 4 Improve Management of OIT Business Functions and Services	Goal 5 Provide Forensic and Scientific Support to CBP’s Law Enforcement and Trade Missions
OIT will continue to operate and maintain the CBP technology infrastructure that supports continuous system availability to provide the services required for successful operation of legacy and new systems and initiatives. While simultaneously improving systems and information availability, OIT will work to achieve efficiencies in operations and maintenance costs.	OIT will streamline and automate the management of the data centers and network environment to maximize the effectiveness of OIT’s limited resources, while enhancing technological availability and ensuring business process continuity.	OIT has a strong commitment to the growth and development of its employees and has created and implemented a leadership and results-oriented performance culture. OIT is developing a human capital strategy to address organizational flexibility and enhanced service delivery while leveraging various opportunities to recruit, retain and manage its talent.	Improved efficiencies will be used to modernize the infrastructure, functions and capabilities that will enable failover, redundancy and availability, increasing reliability and dependability for OIT customers.	Laboratories and Scientific Services provides forensics and trade support to Office of Field Operations, Office of Border Patrol, other offices in CBP, other DHS agencies, and other federal agencies at both the front lines and in the laboratories.

To accomplish these broad goals, the CIO has established specific objectives for each goal with associated key performance indicators. For example, to meet the goal to modernize and transform CBP’s infrastructure, the plan identifies five objectives, including strengthening processes, moving toward the target technical architecture,⁶ and migrating to the Enterprise Data Center.⁷ For each of these objectives, the plan defines key performance indicators that will measure progress toward achieving this goal. The plan also identifies key initiatives related to each goal. For example, initiatives to use cloud-based services, complete field technology upgrades, and migrate systems off of mainframe platforms all contribute to achieving the goal to modernize and transform the infrastructure.

⁶ The target technical architecture is the technical infrastructure that portrays the future or end-state enterprise.

⁷ The Enterprise Data Center initiative encompasses the migration of 24 disparate DHS computing facilities to two geographically diverse, state-of-the-art, and secure enterprise data centers.

The *CBP OIT Strategic Implementation Plan FY 2012–2016* aligns with the goals identified in the DHS and CBP strategic plans. The plan is also aligned with the *DHS Information Technology Strategic Plan 2011–2015* to ensure that CBP OIT supports the DHS CIO’s department-wide IT goals. Table 2 shows the alignment of OIT goals with DHS and CBP goals.

Table 2. Alignment of OIT Goals With CBP, DHS, and DHS CIO Goals

Alignment of OIT Goals with CBP, DHS, and DHS CIO Goals						
CBP OIT		Goal 1: Modernize and transform the infrastructure	Goal 2: Automate the data center and network management environment	Goal 3: Transform and shape the workforce & communications	Goal 4: Reduce costs and improve efficiency	Goal 5: Improve the flow of legitimate cargo and passengers & enforce border security
CBP	Goal 1: Secure the Nation’s borders to protect America from the entry of dangerous people and goods and prevent unlawful trade and travel	✓	✓	✓		
	Goal 2: Ensure the efficient flow of legitimate trade and travel across U.S. borders	✓	✓	✓	✓	✓
DHS	Goal 1: Protect our nation from dangerous people	✓	✓		✓	✓
	Goal 2: Protect our nation from dangerous goods	✓	✓		✓	✓
	Goal 3: Protect critical infrastructure	✓	✓		✓	✓
	Goal 4: Strengthen our nation’s preparedness and emergency response capabilities	✓	✓	✓	✓	✓
	Goal 5: Strengthen and unify DHS operations and management	✓	✓	✓	✓	✓
DHS CIO	Goal 1: Establish secure IT infrastructure capabilities to protect the homeland and enhance our nation’s preparedness, mitigation and recovery capabilities	✓	✓		✓	✓
	Goal 2: Strengthen and unify the department’s ability to share information with federal, state, local and tribal partners	✓	✓		✓	✓
	Goal 3: Improve transparency and accountability through effective governance of cross-departmental IT portfolios		✓		✓	✓
	Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT across the department			✓		

The CIO’s implementation of a well-aligned, up-to-date strategic plan will position OIT to provide effective support to meet mission requirements. An effective IT strategic plan helps focus limited resources and guide the direction of the OIT. If implemented as planned, the IT strategic plan will help CBP personnel fulfill their mission responsibilities.

Enterprise Architecture

The *Clinger Cohen Act of 1996*,⁸ as amended, and OMB circulars⁹ mandate the establishment and use of an enterprise architecture (EA) to guide and direct government investments from inception through retirement. In addition, OMB Memorandum M-11-29, dated August 2011, states that CIOs must use an EA to consolidate

⁸ Public Law No. 104-106, Division E, February 10, 1996. The law, initially titled the *Information Technology Management Reform Act of 1996*, was subsequently renamed the *Clinger-Cohen Act of 1996* in P. L. 104-208, September 30, 1996.

⁹ OMB Circular A-130, Revised, *Management of Federal Information Resources*; and OMB Circular A-11, Revised, *Preparation, Submission, and Execution of the Budget*.

duplicative investments and applications.¹⁰ EA is a management practice designed to maximize the contribution of an agency’s resources, IT investments, and system development activities to achieve mission performance goals.

The CIO has developed an EA to align with the Department’s architecture and guide CBP’s IT environment. The 2010 DHS EA assessment identified CBP’s EA program at stage four of the six stages of the EA Management Maturity Framework.¹¹ CBP’s EA maturity rating was the highest among DHS components. At stage four maturity, an organization has developed an approved version of its EA that is used for targeted results, such as guiding investment decisions. Figure 3 shows CBP’s EA maturity within the stages of the EA Management Maturity Framework.

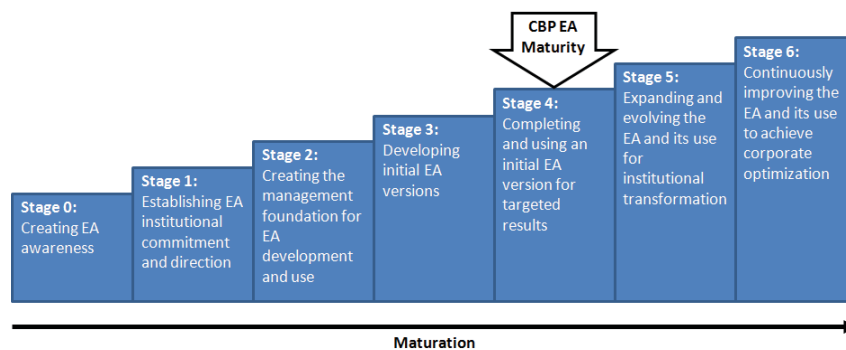


Figure 3. Stages of EA Management Maturity Framework With CBP EA Maturity

As a result of CBP’s progress establishing its EA, the CIO has realized benefits through sharing, reuse, and standardization of IT resources. Specifically, in FY 2011 the EA Branch conducted 20 architecture alignment reviews of investments that resulted in the identification of 90 architecture misalignments. The EA Branch addressed these misalignments through elimination of duplicate efforts and identification of consolidation, integration, and reuse opportunities to realize cost avoidance totaling \$6.1 million. The CIO has also used the EA to eliminate systems that are no longer needed. For example, the EA Branch performed an analysis of border enforcement support systems that identified 16 systems for retirement, some of which were no longer being accessed or had been replaced by newer systems but had not yet been retired.

¹⁰ OMB M-11-29, *Chief Information Officer Authorities*, August 8, 2011.

¹¹ GAO-10-846G, *A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, August 2010.

Development of Target Business Architecture

Although CBP has developed an EA, the EA Branch has not analyzed the “As-Is” business processes to identify efficiencies and fully develop a target “To-Be” view of these processes.¹² The EA Branch is currently building various segments of the “To-Be” view. For example, the EA Branch worked to model “To-Be” process flows for several CBP component offices in 2011. The EA Branch anticipates multiple iterations of the “To-Be” business architecture as various segments are built out.

Progress developing the “To-Be” business architecture has been hindered, in part, by staffing and funding shortages. The EA Branch’s staff of 23 employees falls short of its identified need for 52 employees. Additionally, the EA Branch has absorbed a 50 percent reduction in its operating budget over the past few years. With limited staff and a reduced budget, progress toward establishing the “To-Be” business architecture has been delayed.

Without a complete view of CBP’s target EA, the CIO faces increased risks to efforts to modernize the way OIT provides support to CBP. An EA serves as a critical blueprint that can help ensure that OIT will meet current and future customer needs as the CIO transforms the way OIT does business. For example, an effective “To-Be” architecture can identify potential efficiencies from the elimination of programs that may not align with future mission needs.

Systems Engineering Life Cycle Process

DHS Acquisition Directive 102-01, Appendix B, requires agencies to follow a systems engineering life cycle (SELC) process.¹³ The purpose of the DHS SELC is to establish a standard system life cycle framework across DHS components and to ensure that DHS IT capabilities are delivered efficiently and effectively.

The CBP CIO has implemented the SELC process in compliance with departmental guidance. Specifically, OIT maintains an online process guide, which is CBP’s implementation of the DHS SELC,

¹² Baseline architecture is the set of products that portray the existing enterprise, the current business practices, and technical infrastructure. It is commonly referred to as the “As-Is” architecture. Target architecture is the set of products that portray the future or end-state enterprise, generally captured in an organization’s strategic thinking and plans. It is commonly referred to as the “To-Be” architecture.

¹³ DHS AD 102-01, Interim Version 1.9, *Acquisition Directive*, Instruction Appendix B, November 7, 2008.

called the Enterprise Life Cycle Methodology and Online SELC. This online tool provides a repository of approved project management support processes and procedures, tools, and templates. Figure 4 shows the phases of the DHS SELC and the alignment of CBP’s Enterprise Life Cycle Methodology phases.

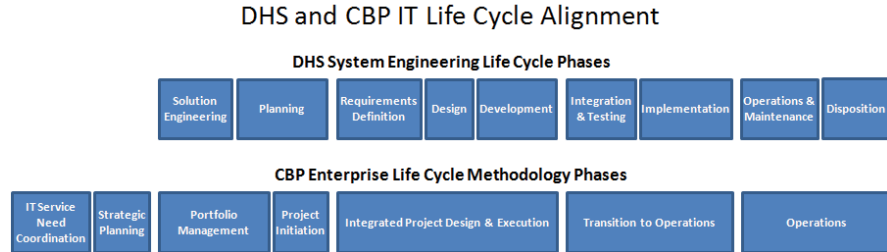


Figure 4. DHS and CBP IT Life Cycle Alignment

CBP has also implemented a governance structure to ensure a level of oversight of IT projects that is appropriate for the size of the investment. IT investments with a life cycle cost of \$300 million and above are considered major acquisitions and are reviewed by DHS. Investments below \$300 million are reviewed within CBP according to three levels. The CBP Executive Steering Committee approves non-major acquisitions with a total life cycle cost from \$50 million to \$300 million. The CBP Governance Board approves non-major acquisitions with a total life cycle cost of \$10 million to under \$50 million. The CBP Enterprise Architecture Review Board approves non-major acquisitions with a total life cycle cost of less than \$10 million. Figure 5 shows the delegation of decision authorities for non-major acquisitions to CBP governance boards based on a program’s life cycle cost.

Lifecycle Cost	Delegation of Acquisition Decision Authority
≥ \$300 million	DHS Acquisition Review Board – Chaired by DHS Deputy Secretary or Under Secretary for Management
\$50 million to < \$300 million	CBP Executive Steering Committee – Chaired by CBP Commissioner and comprised of Assistant Commissioners and Chiefs
\$10 million to < \$50 million	CBP Governance Board – Chair selected by Executive Steering Committee and comprised of CBP Deputy Assistant Commissioners
< \$10 million	CBP Enterprise Architecture Review Board – Chaired by CBP CIO

Figure 5. CBP Decision Thresholds and Decision Authorities for Non-major Acquisitions

OIT’s implementation of the SELC has been effective for several reasons. CBP had a SELC process in place prior to the implementation of Acquisition Directive 102-01 in November

2008. OIT has a history of project management discipline, including the use of its own SELC process, which enabled easier migration of the organization's practices to the DHS SELC process. OIT also had senior executive support and involvement, strong program management, and SELC education and training programs.

In addition to aligning with the DHS SELC, CBP's system engineering governance processes are streamlined and clearly laid out to ensure adherence and compliance. The benefits of this improved process include artifact standardization across programs throughout DHS, reduced risk because of known standard criteria in the internal and external reviews, and the program's ability to meet their scope within schedule and cost. According to the OIT official responsible for the process, all applicable IT projects within CBP go through the SELC process. These IT engineering governance processes enable CBP to make IT investment decisions that will support both CBP and DHS strategic goals.

IT Acquisition Review

DHS MD 0007.1 requires IT acquisitions valued at \$2.5 million or greater to be submitted to the DHS CIO for review. The directive also requires agency CIOs to implement an ITAR process for IT acquisitions below \$2.5 million. ITAR is required before the award of an IT procurement to ensure alignment of acquisitions with IT policy, standards, objectives, and goals across DHS.

The CBP CIO began submitting IT acquisitions valued at \$2.5 million and above to the DHS CIO in FY 2007. That year, the CBP CIO submitted 77 IT acquisitions for review. The number of acquisitions submitted peaked at 198 in FY 2009. The number of IT acquisitions submitted to the DHS CIO for review has declined since FY 2009 due to an overall decrease in new initiative funding, according to OIT officials. Figure 6 shows the number of IT acquisitions submitted to the DHS CIO for review from FY 2007 to FY 2011.

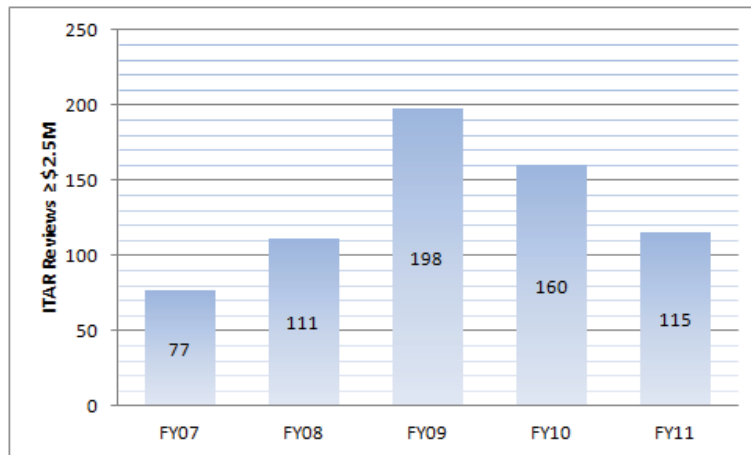


Figure 6. IT Acquisition Reviews \geq \$2.5 Million Submitted to the DHS CIO (FY 2007 to FY 2011)

The CBP CIO has also taken steps to ensure compliance with the ITAR requirement by implementing an ITAR process in FY 2009 to review IT acquisitions with costs below \$2.5 million and above \$1 million. In FY 2009, the CBP CIO reviewed 75 IT acquisitions. The number of ITAR reviews declined in 2011 as new initiative funding has decreased. Figure 7 shows the number of ITAR reviews below \$2.5 million and above \$1 million from FY 2009 through FY 2011.

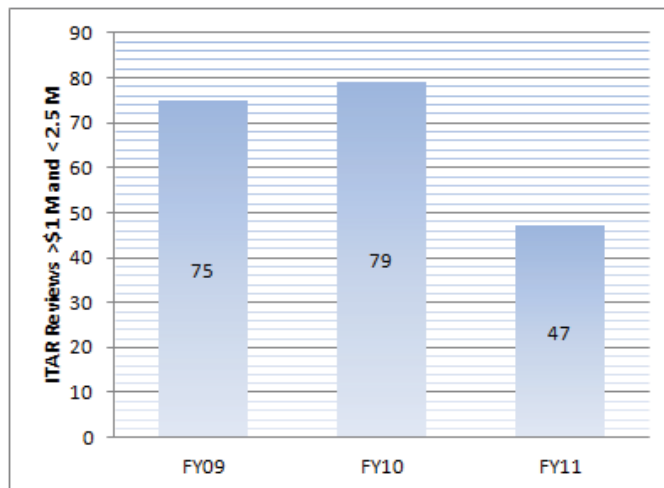


Figure 7. IT Acquisition Reviews Below \$2.5 Million and Above \$1 Million Conducted by the CBP CIO (FY 2009 to FY 2011)

ITAR Compliance

Although the CBP CIO has made progress implementing the ITAR process, not all IT acquisitions that met the dollar threshold and criteria for review have gone through the process. Specifically,

CBP component office IT acquisitions were processed and approved by procurement without going through the ITAR review. OIT personnel run monthly reports to identify procurements that appear to be IT and have been awarded without ITAR review. These reports have identified nearly a dozen acquisitions that were IT related and were awarded without CIO review. For example, OIT personnel have identified IT procurements for human resources systems, financial systems, and border security systems that did not go through ITAR.

Noncompliance with ITAR occurs because CBP component offices do not always follow applicable guidance. According to agency guidance, CBP component offices are required to submit acquisitions that meet the ITAR criteria to the CIO before submitting them to procurement. The CBP Commissioner issued a memorandum in March 2008 to require that CBP component offices comply with the ITAR process. This memorandum instructed CBP component organizations to submit applicable acquisitions to OIT for approval. Since this March 2008 memo, however, compliance challenges remain.

One reason noncompliance remains a challenge for the CIO is the perception that the ITAR process has taken an extended time to complete. During an OIT workshop in FY 2010, the ITAR process was identified as a key process in need of improvement. Specifically, participants at the workshop concluded that ITAR should be redesigned to institutionalize a consistent, enterprise-wide approach to processing IT investment acquisition requests.

OIT has taken a number of steps to improve compliance with ITAR. Specifically, OIT personnel have met with the procurement directorate branch chiefs and the budget officers of other CBP offices to advise them of the ITAR requirement and request their assistance in helping to ensure that all applicable CBP acquisitions follow the process. In addition, OIT personnel reach out to respective CBP component offices to remind them of the process and offer training when noncompliance is identified. Finally, OIT personnel work with CBP component offices to assure them that the ITAR reviews will be processed in a timely manner.

Limitations with ITAR compliance have an impact on the CIO's ability to manage CBP's IT environment effectively. IT acquisition reviews enable the CIO to align IT acquisitions with CBP IT policies, standards, objectives, and goals. ITAR also helps the CIO validate CBP's alignment with the DHS enterprise architecture and

ensure compliance with security and accessibility requirements. However, IT acquisitions that do not go through this process do not go through these alignment reviews and create a risk to CBP's IT environment.

Recommendations

We recommend that the Assistant Commissioner, Office of Information and Technology:

Recommendation #1: Provide the necessary resources to complete required enterprise architecture activities.

Recommendation #2: Implement a plan to ensure the timeliness of the ITAR review process and to communicate this process to component offices and procurement to achieve full compliance.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Commissioner, Office of Internal Affairs. We have included a copy of the comments in their entirety in appendix B.

In the comments, the Assistant Commissioner concurred with our recommendations and provided details on steps being taken to address specific findings and recommendations in the report. We have reviewed management's comments and provided an evaluation of the issues outlined in the comments below.

In response to recommendation one, the Assistant Commissioner concurred and stated that CBP will attempt to provide resources sufficient to complete required enterprise architecture activities. The Assistant Commissioner also provided details about initiatives underway, within the resources currently available, to support enterprise architecture activities effectively. We recognize the establishment of the Transformation Support and Management Group as progress toward a more integrated approach to provided resources to support enterprise architecture development. The Assistant Commissioner requested closure of this recommendation; however, we require additional evidence of the positive impact of actions taken before closing this recommendation.

In response to recommendation two, the Assistant Commissioner concurred and stated that the OIT Financial Management Group would establish outreach efforts, in addition to those already in

place, to achieve full compliance with the ITAR process. We recognize this action as a positive step toward addressing recommendation two. The Assistant Commissioner requested closure of this recommendation; however, we require additional evidence of the positive impact of actions taken before closing this recommendation.

IT Support of Mission Needs

Although the CIO has implemented several key IT management practices, challenges remain in ensuring that the IT environment fully supports CBP's mission needs. Specifically, OIT faces challenges with system availability, including periodic outages of critical security systems. Systems outages have occurred in part because of aging infrastructure, which has not been updated as required because of funding reductions. In addition, the interoperability and integration of the IT infrastructure have not been sufficient to support CBP mission activities fully, due to lengthy requirements gathering and technology insertion processes. As a result, staff have created workarounds and employed alternative solutions to accomplish the mission, including assigning agents to perform duplicative data entry—instead of enforcement duties in the field—and operating stand-alone, non-approved IT. Such activities may hinder CBP's ability to safeguard borders, foster the Nation's economic security through lawful international trade and travel, and ensure officer safety.

Availability and Outages

DHS MD 0007.1 states that the component CIO is responsible for acquiring, developing, operating, and maintaining all mission-related systems and services. In addition, under the *Paperwork Reduction Act of 1995*, as amended, and the *Clinger-Cohen Act of 1996*, as amended, agencies are required to acquire, manage, and use IT to improve mission performance, and plan in an integrated manner for managing their IT architecture.¹⁴

OIT has faced challenges with system availability. Specifically, results from the 2010 OIT Customer Satisfaction Survey indicated that system availability had declined over the prior 2 years. The survey asked CBP component personnel from various offices, including the Office of Air and Marine, the Office of Border Patrol, and the Office of Field Operations, whether system availability had improved, declined, or did not change. The results show increases across these organizations in respondents who said

¹⁴ Public Law 104-13, *Paperwork Reduction Act of 1995*, May 22, 1995.

availability had declined. For example, in 2008, 11 percent of respondents from the Office of Air and Marine indicated that system availability had declined, whereas in 2010 28 percent of respondents indicated that availability had declined. Survey respondents identified several systems that were continuously experiencing availability challenges, such as the Vehicle Primary Client, which processes and documents travelers entering the United States by vehicle at land ports of entry. Figure 8 shows the decline in customer satisfaction with system availability.

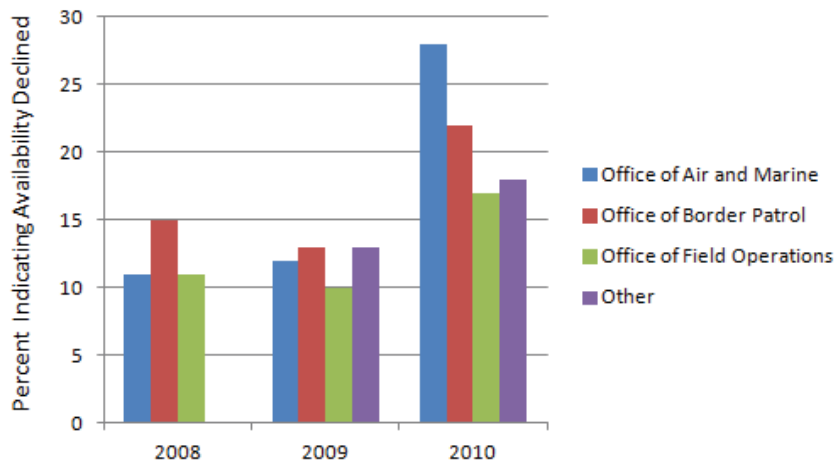


Figure 8. Increase in Customer Dissatisfaction With Availability, From OIT Customer Satisfaction Survey for 2010

Periodic outages of critical security systems, such as the Secure Flight system, have also been reported. Secure Flight is a program that enhances the security of air travel through a streamlined watch list matching process. A report on Secure Flight outages from January to June 2011 identified [REDACTED] outages. Of these [REDACTED] outages, [REDACTED] were related to DHS computer systems managed by CBP, which supports parts of the Secure Flight infrastructure. Some outages were prolonged. For example, [REDACTED]

[REDACTED] OIT determined that the cause of this outage [REDACTED]

Aging Infrastructure

Challenges with systems availability and outages occur in part because of aging infrastructure that has not been updated as

[REDACTED]

required. One high-level OIT official estimated that 70 percent of CBP's infrastructure is more than 4 years old. One part of the infrastructure that has not been updated as required is network components such as servers, routers, and switches.¹⁶ For example, servers are typically replaced every 3 years; however, CBP has a large number of servers that were being used beyond this recommended life cycle. Specifically, at CBP's data center the average age of servers was 6.5 years. Figure 9 shows that only 29 percent of the data center's servers were within the recommended life cycle, while 54 percent were 4 to 7 years old, and 17 percent were 8 to 12 years old.

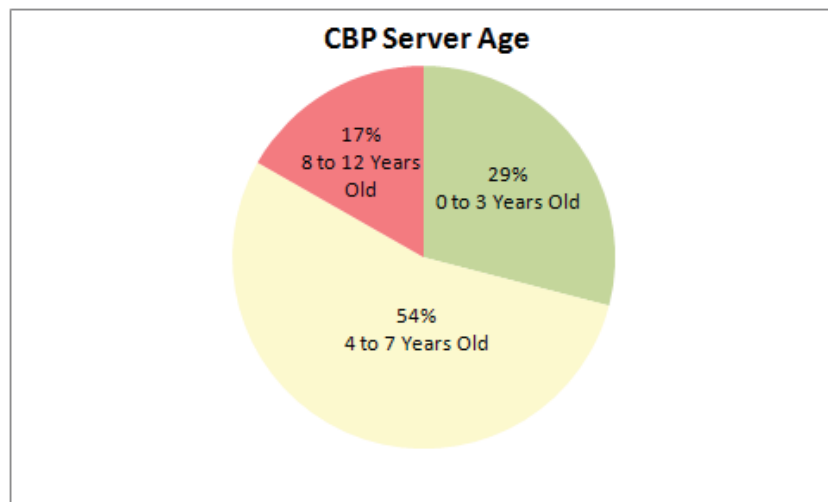


Figure 9. Age of CBP Servers as of December 2011

Similarly, CBP field personnel rely on obsolete network routers and switches. Switches are typically replaced every 5 to 6 years. However, OIT leadership said that CBP has network switches that are 12 to 14 years old.

Certain field personnel also have been using obsolete computers. Some CBP component offices, such as the Office of Border Patrol, have had funding available to replace computers on a 3-year cycle. Other offices, however, such as the Office of Field Operations, have not followed a regular replacement schedule. In several field locations that we visited, IT support personnel had replaced outdated computers with retired Border Patrol computers because they were much newer than the computers still in use by other offices at these locations.

¹⁶ Routers connect a network, acting as dispatchers to choose the best path for information to travel so it is received quickly. A server is a computer dedicated to running one or more services to serve the needs of users of other computers on the network.

Funding for Operations and Maintenance

OIT has not replaced old infrastructure because of funding reductions. Specifically, OIT's budget has been cut by \$335 million since 2009, and further cuts are expected in coming years. CBP has a \$557.8 million investment to maintain CBP's infrastructure across 10 areas, including updating network infrastructure and computers. However, this investment is at risk. The DHS CIO has designated this project as a medium-risk project on the Federal IT dashboard. The Federal IT dashboard assigns major investments a numeric score and a color code associated with the risk level. A score of five is low risk, which is identified as "green," and a score of one is high risk, which is identified as "red." CBP's infrastructure maintenance investment scored a three with a color code of "yellow," associated with a medium-risk project. The assessment of this investment indicated that it is a medium-risk project because of delays caused by limited funding.

OIT leadership has briefed CBP program offices on the risk of outages and the need for CBP to allocate funding toward operations and maintenance to avoid critical interruptions that have an impact on CBP's mission. Maintaining an aging infrastructure is costly, and the CIO plans to reduce overall operations and maintenance costs by modernizing the infrastructure. However, with more budget cuts pending, OIT is reliant on CBP leadership to prioritize funding for maintaining and transforming the infrastructure.

In addition, some field personnel with whom we spoke said that the responsibility for operations and maintenance costs in the field was not always clearly defined. For example, at one field location, Border Patrol personnel had purchased a document management system with the expectation that OIT would cover the operations and maintenance costs. IT field personnel were not authorized or trained to perform database management, and the vendor charged a \$12,000 annual fee for maintenance. Because of the lack of clarity on who was responsible for paying for operations and maintenance, this fee was not paid for several years and, therefore, the maintenance was not performed. Due to the lack of maintenance, this aging system was becoming unstable, and there was a risk that the system would fail and all local Border Patrol documents would be lost.

Reduced IT Support in the Field

Another factor affecting system availability is the reduction in technology field support personnel due to budget cuts. Specifically, as OIT moved toward a centralized help desk structure, field technology support was reduced by 166 personnel, from 785 to 619, in 2009. With reduced numbers, technology personnel in the field had difficulty supporting numerous geographically dispersed sites that may be hard to access. For example, in some areas in the Northwest it can be an all-day drive for technology field support personnel to get to a site. Furthermore, some locations have a small number of technology support personnel to cover a large area, which can lead to downtime if multiple sites need support simultaneously.

In addition, as field operations expanded there was often no commensurate expansion of IT support. For example, at a new Border Patrol facility in Tucson, intelligence personnel lost information because IT field support personnel did not verify that 30-day server backups were occurring. Intelligence officers had to recreate numerous reports on organizations and individuals being targeted, such as smuggling organizations. The manager of this office said that this mistake would have been avoided with a dedicated IT support person. When this new facility was created, however, additional resources for technology support were not factored in, and technology support personnel in this sector were stretched too thin. The field IT support personnel said that they are in a reactive mode of fixing what breaks, whereas the goal should be to be proactive.

Bandwidth

Increasing demand for bandwidth has also contributed to system availability challenges. Commercial network providers do not offer service in many of the areas where CBP operates; consequently, it is costly to provide adequate bandwidth in some areas. In addition, CBP is transitioning mainframe systems to web-based systems. For example, TECS and ACE, two of CBP's largest enterprise systems, are being modernized and moved off of the mainframe. Demand for bandwidth increases as more applications become web-based. As a result, CBP personnel in areas with limited bandwidth have increased difficulty accessing required systems.

As a result of availability challenges and outages, CBP faces critical impediments to achieving its border security, trade, and travel missions effectively. For example, for every hour of downtime, 46,000 people and 3,000 containers back up at the borders, seaports, or airports during normal operations; during peak hours as many as 120,000 people may be affected. A nationwide passenger outage of more than 2 hours would cause significant problems for air travel and land borders, and a 1-day nationwide outage affecting cargo would have national economic consequences. This was evident on August 11, 2007, when a network outage at the Los Angeles International Airport prevented CBP from conducting its normal operations for approximately 10 hours and affected more than 17,000 passengers.

Interoperability and Functionality

OIT faces challenges with external interoperability and internal functionality. Specifically, in some regions, CBP employees do not use digital radio communications or have access to websites and software provided by external partners. In addition, enterprise-wide systems do not meet all CBP users' requirements, such as for internal reporting, needed to support CBP's mission.

External Interoperability

Office of Border Patrol staff cannot communicate seamlessly with Federal, State, and local partners in all sections of the country. Specifically, staff in some regions are using analog radios, which creates communications barriers with partners such as the U.S. Coast Guard and local, county, and State law enforcement organizations. For example, in 2009, CBP agents in one location were unable to share information with the U.S. Coast Guard through a secure mode for approximately 3 to 6 months. When the U.S. Coast Guard switched from analog communications to digital communications, CBP staff in the region lost the ability to share encrypted information with the U.S. Coast Guard. Once notified of the inability to communicate securely, CBP field technicians resolved the issue by programming the radios to allow communication between the two agencies. Had there been an emergency situation, however, staff would not have been able to communicate effectively. According to CBP OIT field support staff, this interruption in communication could have been avoided if standard methods of notifications for changes to tactical communications had been available.

In addition, CBP faces communication challenges with State and local partners in some regions. Specifically, in some regions, key partners use digital communications, while Border Patrol agents in the same communities may use analog communications. After September 11, 2001, State and local officials' radios switched to digital communications. However, Office of Border Patrol staff in some regions cannot communicate with radios at that frequency. In these regions, State and local interoperability is provided by the use of two portable radios and a direct line to a dispatch center at the Office of Border Patrol. For example, in one location a Border Patrol agent on duty in the field might reach out to local law enforcement for assistance and backup support. Without digital radio communications, the agent must use the dispatch center to connect to the local law enforcement office for assistance. Staff reported that communicating through the dispatch center is not always feasible because it requires an open line, and it takes longer than using direct digital radio communications. The use of two portable radios for communication between Border Patrol and other partners also has challenges. If an agent forgets the Border Patrol radio, the agent cannot keep the home office informed of his or her needs, and local law enforcement must call the Border Patrol office to let it know, for example, when the officer is in pursuit.

The current radio environment in certain regions contributes to officer safety challenges and threats to security around the Nation's borders. Analog radio communication in some regions is unencrypted, which may result in unsecure communications. While the dispatch center aids in communication, it is not an ideal environment for mission operations. For example, staff at one Border Patrol sector described an environment in which dispatchers, trained to operate multiple phones simultaneously and to cover the entire State and partners such as the U.S. Coast Guard, may "burn out." Border Patrol staff then must train additional staff to work in the dispatch center. In addition, staff with whom we met agreed that scrambling to find a radio to contact the office might distract an agent from enforcement and surveillance activities. Further, if the dispatch connection were to go down, the agent might be disconnected from sufficient outside support.

Office of Air and Marine staff with whom we met reported challenges in accessing the government and military-issued web sites they need to accomplish their missions. For example, they reported being unable to access critical government web sites necessary for mission activities such as setting up a flight plan. Such web sites include the National Geospatial Intelligence

Agency web site, Army Knowledge Online, the Joint Technical Data Integration web site, and aviation weather web sites. In addition, Air and Marine staff reported being unable to use key software necessary for planning routes, charts, and flights, as well as aircraft maintenance for select aircraft, because the software was not on the approved technology list.

As a result, the Office of Air and Marine staff set up stand-alone computers to view the inaccessible web sites and to install the military software to meet their needs. Stand-alone computers may create security, integration, and maintenance challenges. OIT Field Technology Officers cannot maintain IT that is not on the approved list. Therefore, if a non-approved IT product breaks, OIT staff are not authorized to fix it. Non-approved technology creates security challenges. In addition to operating stand-alone computers, staff may place non-approved IT on the network without realizing that the information could be compromised. Since non-approved technology has not been approved or tracked by OIT, Information Systems Security Officers throughout CBP may not be aware it exists, and it could compromise network security.

Internal Functionality

CBP staff face challenges in transferring and sharing data locally or internally as well. For example, Office of Air and Marine staff said that they needed to transfer unencrypted data from the aircraft digital video recorders onto computers, where it can be shared on the network for evidence and intelligence purposes. Because DHS policy prevents the use of portable media devices, staff obtained a waiver to transfer unencrypted data from the aircraft to network computers. In addition, the agency bought approximately 20 scope trucks at an estimated \$450,000 each for Border Patrol offices. Border Patrol agents in one region reported that an agent using a scope truck in the field can view live video from the truck's mobile video surveillance system, which includes two cameras. However, the video feed cannot be recorded or sent over the network. Therefore, agents cannot view the feed from the command center or use it as evidence.

In addition, some enterprise systems and applications do not include the reporting functionality that users need at the field component or program level. For example, E3, an enterprise-wide system, does not capture the information that field personnel need on the form generated for each illegal alien transported through the

Alien Transfer Exit Program. Approximately seven Border Patrol sectors in the Southwest are involved with this program. To overcome this system limitation, since December 2010, agents in one sector have entered identical information each day pertaining to hundreds of individuals into both E3 and Excel in order to produce the required reports that E3 alone cannot produce. The reports include lists of transferred illegal aliens and other information that helps CBP determine the most effective operations. According to a site supervisor, multiple entry may increase the possibility of data integrity issues. Furthermore, when agents spend time reentering data, they are not spending that time on other duties, such as enforcement activities in the field.

The Border Patrol Enforcement Tracking System (BPETS), an enterprise-wide system, also does not sufficiently meet the local reporting needs of field components. Specifically, staff in one sector have implemented duplicate and even triplicate reporting at the local level for some functions, including checkpoint activity reports, scheduling reports, zone activity reports, and intelligence reports. OIT staff reported that the input fields within BPETS were too restrictive to provide the level of reporting that local managers needed for planning and oversight, and that the system did not generate useful, consolidated reports. As a result, agents at these stations spent time duplicating or augmenting the required information for locally generated reports, using time that could be spent in direct support of enforcement duties or personnel management.

Requirements and Technology Insertion

OIT has established a requirements gathering process, but it does not fully support mission needs and is unclear to some staff with whom we met in the field. Each program office within OIT, such as the Border Enforcement and Management Systems Program Office, the Wireless Systems Program Office, and the Passenger Systems Program Office, has its own processes for meeting its customers' needs and prioritizing requirements. CBP IT leadership noted challenges with the requirements process, including the length of time it takes to compile and implement requirements. Field staff with whom we met were sometimes unclear on how to share requirements or were not sure that their voices were being heard. For example, field staff might send a request, including what they need and why they need it, "up the chain" or through OIT. But staff with whom we met, including OIT staff, were not uniformly convinced that the process moved

forward.

OIT has also established a process for customers to request approval for new technology if a gap between a business need and the existing list of approved IT is identified. CBP's Technical Reference Model contains the status of IT products and the degree to which CBP customers can use them. Customers may initiate requests for new technology through the Intranet. Upon reviewing and researching a customer's request, OIT staff may approve the request and add the IT product to the Technical Reference Model. OIT staff in the field, however, reported that the technology insertion process was not an easy or quick process. One representative from OIT leadership said that it took 4 months to add new products to the Technical Reference Model. In addition, a customer may request that specific software be installed, but when field support staff search the Technical Reference Model, the version that is listed is one to two versions old. Staff said that the list was not consistently current and kept up to date, and that newly approved software might not be on the list.

CBP is taking steps to improve the requirements process. Specifically, OIT has created governance boards to address and streamline requirements, which is critical to resolve emergencies, reduce redundant efforts, and identify priorities. For example, matters deemed to be emergencies, such as issues affecting officer safety, are resolved through processes established by the OIT Change Control Board. OIT has established the Customer Entry Point Governance Board, composed of senior executives from each OIT division, to review major OIT efforts and reduce duplication of efforts. Further, OIT has created the Requirements Management User Group in an effort to standardize the process for the management of requirements throughout OIT.

In addition, OIT has initiated outreach activities to operational components. In October 2011, OIT leadership briefed key CBP offices on the status of OIT, during which staff learned about transformation efforts and the need for operational components to prioritize needs before providing them to OIT. In addition, OIT held monthly outreach meetings with the Office of Border Patrol, the Office of Air and Marine, the Office of Human Resources Management, the Office of Field Operations, and the Office of International Affairs. During these meetings, staff from these operational components brought forward IT issues and concerns, which were then tracked as they were resolved.

As a result of IT not completely meeting user needs, CBP employees have created workarounds or employed alternative solutions that may have an impact on the agency's ability to protect its frontline officers, secure the Nation's borders, and ensure lawful trade and travel. Unsecured and insufficient communication can create safety risks for agents, officers, and other frontline staff. In addition, integration and interoperability gaps, such as the use of stand-alone computers or systems that do not communicate with each other, can lead to missed links and opportunities to gather the critical intelligence necessary to prevent illegal entry into the United States; stop terrorists and drug smugglers; and foster safe, legitimate trade and travel.

Recommendations

We recommend that the Assistant Commissioner, Office of Information and Technology:

Recommendation #3: Develop a funding strategy to ensure replacement of outdated infrastructure in order to address availability challenges and outages.

Recommendation #4: Implement a plan to address gaps in the existing requirements and reassess the technology insertion process to address functionality and interoperability challenges in the field.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Commissioner, Office of Internal Affairs. We have included a copy of the comments in their entirety in appendix B.

In response to recommendation three, the Assistant Commissioner concurred and said that CBP has been working on an initiative to respond to the infrastructure needs of the Office of Field Operations, the Office of Border Patrol, and the Office of Air and Marine. He also said that CBP has been reporting on this initiative in response to a prior recommendation from our February 2011 report, *Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project*. Our current report's finding and recommendation, however, go beyond the scope of the 2011 report, which focused on CBP's planning to reduce the risk of outages at border stations and ports of entry in the field. This report addresses availability challenges with network infrastructure in the field, as well as at headquarters.

Therefore, we do not agree that the June 2011 strategy for replacing outdated infrastructure is sufficient to address this recommendation. Before closing this recommendation, we require additional evidence of a funding strategy to address CBP's challenges with outdated infrastructure in the field as well as at headquarters.

In response to recommendation four, the Assistant Commissioner concurred with the recommendation and stated that CBP has already taken action to increase automation of the technology insertion process. Further, the Assistant Commissioner said that the OIT Chief Technology Officer agreed to reassess the automated implementation as part of an annual process review. We recognize this action as a positive step toward addressing this recommendation. This recommendation will remain open pending evidence of further progress in this regard.

Appendix A

Purpose, Scope, and Methodology

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted an audit to evaluate the CBP CIO's overall IT management approach, including the extent to which IT management practices have been put in place and the current IT environment supports mission needs.

We researched and reviewed Federal laws, management directives, and agency plans and strategies related to IT systems, management, and governance. We obtained published reports, documents, and news articles regarding CBP's management and use of IT. Additionally, we reviewed recent Government Accountability Office and DHS OIG reports to identify prior findings and recommendations. We used this information to establish a data collection approach that consisted of focused interviews, documentation analysis, site visits, and system demonstrations to accomplish our audit objectives.

We held interviews and teleconferences with CBP staff at headquarters and field offices. Collectively, we held more than 60 meetings with headquarters officials, field office officials, and system users to learn about CBP's IT functions, processes, and capabilities. At headquarters, we met with CBP OIT officials including the Deputy Assistant Commissioner, Chief Technology Officer, branch chiefs, and program managers to discuss their roles and responsibilities related to CBP IT management. We also met with staff from OIT program offices, including the Passenger Systems Program Office, Cargo Systems Program Office, Wireless Systems Program Office, Border Enforcement and Management Systems Program Office, and Targeting and Analysis Systems Program Office.

At CBP field locations, we met with senior managers, area service managers, field technology supervisors, field technology officers, import specialists, agents, pilots, port directors, and other system users to understand IT development practices, user requirements, and system use in the field. We discussed the current IT environment and the extent to which it met mission needs, local IT development practices, and user involvement and communication with headquarters. We collected supporting documents about CBP's IT environment, IT management functions, current initiatives, and improvement initiatives.

Appendix A

Purpose, Scope, and Methodology

We conducted audit fieldwork from October 2011 to January 2012 at CBP headquarters offices in Washington, DC. We conducted additional audit fieldwork at CBP field offices and operational sites.

We conducted this performance audit between October 2011 and April 2012 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Richard Harsche, Director of Information Management. Major OIG contributors to the audit are identified in appendix C.

Appendix B

Management Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229



**U.S. Customs and
Border Protection**

May 22, 2012

Mr. Frank Deffer
Assistant Inspector General
Information Technology Audits
Department of Homeland Security
245 Murray Drive, SW, Building 410
Washington, DC 20528

Re: OIG Draft Report Entitled, "CBP Information Technology Management: Strengths and Challenges," (OIG-10-135-ITA-CBP)

Dear Mr. Deffer:

Thank you for the opportunity to review and comment on this draft report. The U.S. Customs and Border Protection (CBP) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this important report.

While the report notes the maturity of CBP's Enterprise Architecture (EA) it questions the movement towards a target architecture. In order to achieve that goal, the CBP Chief Information Officer (CIO) has already approved a Target Business Architecture which aligns with the U.S. Department of Homeland Security (DHS) Management Directive (MD), DHS MD 0007.1 and the Information Technology Infrastructure Library (ITIL) v3 framework and directly supports the DHS CIO High Priority Initiatives for transforming DHS. The CBP CIO recognizes this is a major business transformation initiative; therefore, the CIO recently established the CBP Office of Information Technology (OIT) Transformation Support and Management Group (TSMG). This group is charged with enabling the OIT transformation to ensure that our workforce is prepared to adapt to technology and business practice transitions. The TSMG is working with the Enterprise Architecture Branch, Financial Management Group, Workforce Management Group, Chief Technology Office (CTO) and a number of other OIT offices to coordinate on activities that are necessary to move OIT forward as an organization.

In addition to the work being performed by OIT's Enterprise Architecture Branch, CBP has adopted a federated architecture model, where the CBP CTO is responsible for the Information Technology (IT) Transformation Initiatives, including the Technology Strategy, Technology Roadmap, IT Governance, Technology Lifecycle, and the CBP architecture framework. This architecture model aligns component architectures and is based on open standards and industry best practices, while remaining technology agnostic. The goal of this comprehensive approach to architecture and innovation is to serve the mission by providing innovative technology services and solutions for designing and building infrastructure and business applications.

Appendix B

Management Comments to the Draft Report

2

These solutions are highly reliable, available, scalable, and perform at a level that enable CBP agents and officers to meet their mission objectives 24 hours a day, seven days a week.

CBP agrees with the description of the Systems Engineering Life Cycle Process (SELC) in the report but wishes to add that CBP is working with DHS on two Agile-methodology initiatives which further streamline the process. The DHS CIO created an Agile Integrated Product Team (IPT) to explore ways to further the use of the Agile methodology. CBP also has a Service Oriented Architecture (SOA) initiative which recently facilitated the development, in 45 days, from concept to production of an important law enforcement tool.

CBP also agrees that the report highlights the challenges associated with aging and legacy infrastructure but would like to note some of the initiatives underway to address these challenges. Among the responses to these challenges are the Common Delivery Platform (CDP) and the Common Cloud Computing Environment (C3E).

The objective of the CDP initiative is to focus on adopting technology standards that help avoid vendor lock-in, highly specialized skill sets, and higher licensing fees. This reason makes adoption of standards-based Common Infrastructure a compelling choice for CBP. CDP eliminates single-point-of-failure across all layers of the application stack: Network, Web, Application, Database, and Storage by supporting Active/Active, geographically diverse applications and infrastructure. CDP drastically reduces engineering costs and time-to-market by standardizing applications on a common infrastructure footprint and preventing technology refresh stovepipes by upgrading the application infrastructure system as a whole.

The CBP C3E initiative is being implemented to provide an integrated, enterprise-wide common infrastructure platform to adhere to the architecture guidelines of CBP CDP.

The main goal of C3E is to provide the following enterprise-wide services:

- Application & Database Capacity Planning
- Automated Geographic Failover & Failback
- Automated Patching
- Centralized Performance & Availability Monitoring
- High Speed Backup & Recovery
- Just-In-Time Environment Provisioning
- Service Level Agreement (SLA) Management & Reporting.

CBP agrees with the challenges described with attaining external interoperability and internal functionality. Improvements are underway. For instance, the example of the 20 scope truck lacking functionality was caused in part because initially this effort was not categorized as an IT effort and therefore did not go through the rigor of the SELC which would have required a clearer understanding of the functional requirements. These and similar efforts will be categorized as IT and comply with the SELC.

In the area of wireless technology DHS has established an enterprise change management process that all technology managers within DHS are required to follow when making significant changes to a system. To help combat these types of communication challenges,

Appendix B

Management Comments to the Draft Report

3

DHS has established an enterprise wide Joint Wireless Program Management Office (JWPMO) that will help improve tactical communications (TACCOM) among DHS components.

CBP OIT's Wireless System Program Office (WSPO) has initiated a large scale project that will convert all remaining Land Mobile Radio (LMR) sites to digital. This project is known as the "Digital-In-Place (DIP)" project. WSPO is working closely with the Office of Border Patrol (OBP) along with other key stakeholders within CBP to carefully assess what equipment and deployment services are required for each existing analog LMR site. The current plan begins with the conversion of the mission critical sites to digital in the 2012/2013 timeframe. It is estimated that all sites will be converted to digital within the 2014/2015 timeframe.

As for the computer programs, suggestions for revisions to the e3 Processing related to the I-216 form have been identified by the OBP and Phase 1 of those changes are underway and will be in place in May 2012. The changes should ease sector data entry burdens eliminating any decisions by sectors to enter the data separately in spreadsheets. OIT is working with the OBP to replace legacy Border Patrol Enforcement Tracking System (BPETS) with a modernized solution, BPETS2. The first release of BPETS2, implemented in March 2012, replaced legacy BPETS staffing and scheduling functionality and should have addressed any reporting deficiencies perceived by the sectors in the scheduling area. Future releases of BPETS2 will modernize other areas of BPETS as prioritized by OBP.

To meet the challenges of requirements and technology insertion (TI), since August of 2010 the TI process has become automated and paperless through the use of SharePoint. It is possible that some of those interviewed for the report were unaware of this change and were recalling a slower moving TI process. Using the improved process, OIT was able to complete 430 TIs in FY 2011. While this tempo is jeopardized by recent budget reductions, every effort will be made to maintain responsiveness to requests. The Technology Reference Model (TRM) is now required to be updated within 5 business days. OIT is routinely updating the TRM with 2 business days. This should facilitate the responsiveness of OIT Field Support personnel to customer requests.

The OIG made four recommendations to the Assistant Commissioner, Office of Information and Technology/Chief Information Officer to provide needed resources for enterprise architecture activities, ensure compliance with the information technology acquisition review process, develop a funding strategy for the replacement of outdated infrastructure, and reassess the existing requirements and technology insertion processes to address challenges in the field. CBP concurs with all four recommendations.

Recommendation 1: Provide necessary resources to complete required enterprise architecture activities.

CBP Response: CBP concurs with the recommendation and will attempt to provide resources sufficient to complete required enterprise architecture activities. Within the resources currently available, a cross organizational team has already been formed to take an integrated approach to providing resources to support enterprise architecture. The Transformation Support and Management Group (TSMG) is working with Chief Technology Office, the Enterprise Architecture Branch, the Financial Management Group, the Workforce Management Group, and a number of other OIT offices to coordinate on activities that are necessary to move OIT forward as an organization.

Appendix B

Management Comments to the Draft Report

4

The TSMG was formed on April 3, 2012. As the attached evidence shows, this is an effort to use currently available resources to address enterprise architectural needs until funding permits adding resources. CBP respectfully requests closure of this recommendation.

Recommendation 2: Implement a plan to ensure the timeliness of the ITAR review process and to communicate this process to component offices and procurement to achieve full compliance.

CBP Response: CBP concurs with the recommendation. Despite having performed outreach to many CBP organizations more communication and training is necessary. The OIT Financial Management Group will work to establish additional outreach efforts to further alert and educate the CBP acquisition community on the Information Technology Acquisition Review (ITAR) requirement for all CBP-wide IT-related acquisitions.

As the attached May 16, 2012, evidence from the CBP intranet site demonstrates, efforts have been renewed to achieve full compliance with the ITAR. This effort is an ongoing activity. CBP respectfully requests closure of this recommendation.

Recommendation 3: Develop a funding strategy to ensure replacement of outdated infrastructure in order to address availability challenges and outages.

CBP Response: CBP concurs with the recommendation. CBP notes that this recommendation is similar to a recommendation from another OIG report entitled, "Planning and Funding Issues Hindered CBP's Implementation of the System Availability Project," (OIG-11-42). Pursuant to that review, CBP is reporting progress to the OIG on a ten year initiative to respond to the infrastructure needs of the Office of Field Operations, Office of Border Patrol and Office of Air and Marine. The goal is to ensure end-to-end network connectivity and high rates of network availability; reduce single points-of-failure within the CBP infrastructure; establish a continuous technology refresh lifecycle for key hardware network and software network components; forecast technology advances and alignments to CBP/OIT strategic objectives and the lines of business of the CBP key stakeholders. CBP will continue to provide status updates to the OIG on the funding and execution of the plan.

Since the strategy for replacing outdated infrastructure has existed since June 2011 and its progress is being tracked under a separate OIG audit, CBP respectfully requests closure of this recommendation.

Recommendation 4: Implement a plan to address gaps in the existing requirements process and reassess the technology insertion process to address functionality and interoperability challenges in the field.

CBP Response: CBP has already taken action to increase automation of the technology insertion (TI) process. As the owner of the TI process the OIT/CTO agrees to reassess the automated implementation and over-arching process as a part of an annual process improvement review. The first review will be completed by Dec 31, 2012.

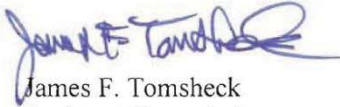
Appendix B
Management Comments to the Draft Report

5

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments have been provided to the OIG under separate cover.

We look forward to working with you on future reviews. If you have any questions, please have a member of your staff contact Patty Quintana, Audit Liaison, Office of Internal Affairs at (202) 325-7711.

Sincerely,



James F. Tomsheck
Assistant Commissioner
Office of Internal Affairs

Attachments

Appendix C
Major Contributors to This Report

Richard Harsche, Division Director
Steven Staats, Audit Manager
Elizabeth Argeris, Auditor-In-Charge
Swati Nijhawan, Auditor-In-Charge
Erin Dunham, Auditor
Sheila Cuevas, Auditor
Anthony Nicholson, Referencer

Appendix D
Report Distribution

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
CBP, Commissioner
CBP, Deputy Commissioner
CBP, Assistant Commissioner, Office of Information and
Technology
CBP 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 e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to Department of Homeland Security programs and operations:

- Call our Hotline at 1-800-323-8603
- Fax the complaint directly to us at (202)254-4292
- E-mail us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigation - Hotline,
245 Murray Drive SW, Building 410
Washington, DC 20528

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