OFFICE OF INSPECTOR GENERAL

CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations

Homeland Security

September 28, 2017
OIG-17-114

DHS OIG HIGHLIGHTS

CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations

September 28, 2017

Why We Did This Audit

Information technology (IT) is a critical asset to support U.S. Customs and Border Protection's (CBP) mission operations. We conducted this audit to assess the effectiveness of IT systems to support the accomplishment of CBP's border security objective of preventing the entry of inadmissible aliens who may pose threats to national security.

What We Recommend

We made seven recommendations to address CBP's passenger screening and border security IT systems and infrastructure challenges.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

CBP's IT systems and infrastructure did not fully support its border security objective of preventing the entry of inadmissible aliens to the country. The slow performance of a critical pre-screening system greatly reduced Office of Field Operations officers' ability to identify any passengers who may represent concerns, including national security threats. Further, incoming passenger screening at U.S. international airports was hampered by frequent system outages that created passenger delays and public safety risks. The outages required that CBP officers rely on backup systems that weakened the screening process, leading to officers potentially being unable to identify travelers that may be attempting to enter the United States with harmful intent.

IT systems and infrastructure also did not fully support Border Patrol and Air and Marine Operations border security activities between ports of entry. Poor systems performance and network instability hampered these CBP operations nationwide. This resulted in excessive processing backlogs and agents' inability to meet court deadlines for submitting potential alien criminal prosecution cases. Also, frequent network outages hindered air and marine surveillance operations, greatly reducing the situational awareness needed to detect inadmissible aliens and cargo approaching U.S. borders. CBP has not yet addressed these long-standing IT systems and infrastructure challenges, due in part to ongoing budget constraints.

Management Response

CBP concurred with our recommendations.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 28, 2017

MEMORANDUM FOR: Phillip A. Landfried
Assistant Commissioner
Office of Information and Technology
U.S. Customs and Border Protection

FROM: Sondra F. McCauley
Assistant Inspector General
Information Technology Audits

SUBJECT: *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations*

Attached for your action is our final report, *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations*. We incorporated the formal comments provided by your office.

The report contains seven recommendations to address CBP's passenger screening and border security IT systems and infrastructure challenges. Your office concurred with all seven recommendations.

Based on information provided in your response to the draft report, we consider recommendations 1 through 7 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Kristen Bernard, Director, Information Technology Management, at (202) 254-0962.

Attachment

Table of Contents

Appendixes

Abbreviations

AMO	Air and Marine Operations
AMOSS	Air and Marine Operations Surveillance System
APIS	Advance Passenger Information System
ATS-QQ	Automated Targeting System – Quick Query
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
e3	Enforce 3
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IT	information technology
OFO	Office of Field Operations
OIG	Office of Inspector General
OIT	Office of Information and Technology
PALS	Portable Automated Lookout System
TPAC	Traveler Primary Arrival Client

Background

U.S. Customs and Border Protection (CBP), the front-line border protection agency within the Department of Homeland Security, is responsible for securing the U.S. borders and facilitating lawful international travel and trade. CBP plays a crucial role in enforcing laws and regulations related to immigration and border security, intercepting malicious criminals and materials, and maintaining domain awareness to prevent terrorist attacks. CBP is one of the world's largest law enforcement organizations, with 60,000 officers, agents, and support personnel nationwide. In fiscal year 2017, CBP's total budget was approximately $13 billion, accounting for 21 percent of DHS' total budget of approximately $66.8 billion. According to CBP, on a typical day its employees:

- process more than 1 million passengers and pedestrians,
- process more than 280,000 incoming vehicles,
- conduct more than 1,100 border apprehensions,
- arrest more than 20 wanted criminals at ports of entry,
- refuse entry of more than 750 inadmissible persons, and
- conduct more than 290 hours of air and sea enforcement missions.

CBP's primary immigration enforcement mission at ports of entry is to confirm eligible travelers and exclude inadmissible foreign nationals from entering the United States. CBP takes a comprehensive approach to safeguarding the border by combining customs, immigration, and border security into one coordinated effort. This border security mission is accomplished by officers and agents located within the following three CBP offices.

Office of Field Operations (OFO) – OFO is the law enforcement entity responsible for immigration inspections at U.S. ports of entry. More than 22,000 OFO officers conduct inspections at 241 U.S. international airports, 110 land ports of entry, and 126 sea ports of entry. To manage these ports of entry, CBP has 20 field operations offices strategically located throughout the country.[1]

U.S. Border Patrol (Border Patrol) – The U.S. Border Patrol is CBP's primary law enforcement organization, responsible for preventing the entry of inadmissible aliens, including criminals and terrorists, as well as contraband between U.S. ports of entry.[2] Agents protect the country each day by patrolling more than 5,000 miles of border with Canada, 1,900 miles of border with Mexico, and 95,000 miles of shoreline. Border Patrol

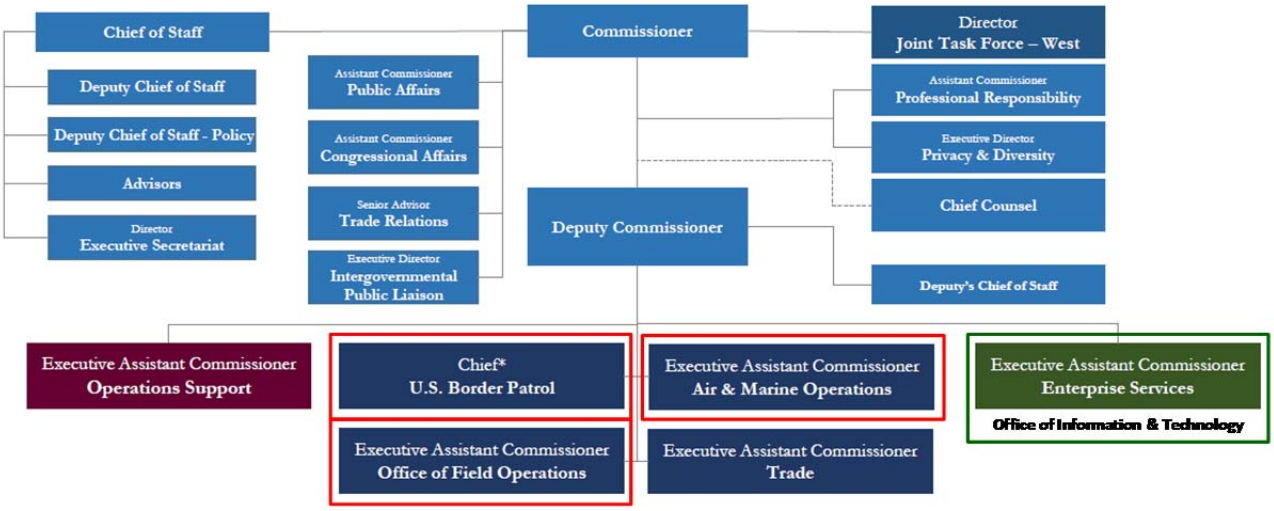
[1] Ports of entry are facilities that provide for travelers' controlled entry into, or departure from, the United States.
[2] An illegal alien is a foreign national who is an unauthorized resident of the host country in which he or she is residing.

agent protection operations include conducting watch along the border, traffic inspections at checkpoints along highways leading from border areas, city patrol and transportation checks, and anti-smuggling investigations. These operations are carried out across 35 checkpoints, 135 border patrol stations, and 20 substations nationwide. CBP has divided geographic responsibility for U.S. border security operations among 20 border patrol sectors along the southwest, northern, and coastal borders.

Air and Marine Operations (AMO) – AMO agents provide air and sea defense of the Nation's land and sea borders by intercepting inadmissible aliens and cargo approaching U.S. borders. Approximately 1,800 AMO agents maintain 240 aircraft and 300 marine vessels operating throughout the United States, Puerto Rico, and the U.S. Virgin Islands.

These three offices are depicted in the boxes outlined in red in figure 1.

Figure 1: CBP's Organizational Structure as of June 2016



Source: Office of Inspector General (OIG)-generated based on CBP data

Technology Is Critical to Support CBP's Border Security Operations

Information technology (IT) is a critical asset to facilitate and enhance CBP's complex mission operations. The CBP Assistant Commissioner of the Office of Information and Technology (OIT) provides infrastructure, technology, and communications to carry out border security operations.[3] OIT field support

[3] The CBP Assistant Commissioner of the Office of Information and Technology is also CBP's Chief Information Officer (CIO).

personnel provide day-to-day technical assistance to more than 1,400 CBP locations nationwide. OIT manages all IT networks, computers, systems, data, tactical communications, and other essential resources to support CBP's 60,000 employees. In addition, OIT provides full-scale IT systems research, development, testing, implementation, maintenance, training, and support services. In FY 2016, CBP's IT budget of $1.4 billion was the largest within DHS, comprising about 23 percent of the Department's $6.2 billion IT budget. OIT has more than 5,200 IT staff, including 1,953 Federal employees and 3,280 contractors, supporting CBP's IT environment.

OIT implements and supports numerous mission-critical systems and tools that deliver essential capabilities for 24/7 border security mission operations. Table 1 lists the primary systems used to support each distinct border security mission area.

Table 1: Selected Border Security Systems by CBP Mission Area

OFO Immigration Inspections and Screening Systems	
TECS (not an acronym)	TECS is the principal information sharing platform that allows OFO personnel to access numerous applications and databases supporting border enforcement operations. OFO uses a TECS Portal to input or access law enforcement, inspection, and intelligence records, referred to as "lookouts." OFO officers can query TECS to search for a traveler, by name or other biographic fields, against law enforcement and national security watchlists to identify possible concerns, such as prior CBP violations or other infractions of law. OFO officers also use TECS to record and report on primary and secondary inspection results, generally referred to as TECS Records. Additional inspection and screening applications reside on the TECS platform: • Traveler Primary Arrival Client (TPAC) – TPAC is the primary passenger screening module used to process, document, and confirm the identity of international travelers at air and sea ports of entry. TPAC interfaces with the Office of Biometric Identity Management's Automated Biometric Identification System (IDENT), used to collect biometric data, such as fingerprints and photographs, from non-citizen travelers. IDENT also verifies the identity of a traveler to determine whether the person is using an alias or fraudulent identity. This is done via an automated query that compares the traveler's biographic information against biometric records in IDENT. • Automated Passport Control – Eligible travelers use this self-service kiosk during the primary inspection process to scan their passports, take photographs, and answer a series of questions that verify their biographic and flight information. The kiosk issues receipts, which the travelers provide, along with their passports, to OFO officers to finalize the inspection process. • Global Entry – This self-service kiosk expedites the inspections process for pre-approved, low-risk travelers. Using this kiosk, travelers scan their passports or U.S. permanent resident cards, submit their fingerprints, and

OFO Immigration Inspections and Screening Systems	
	complete their customs declarations. • Advance Passenger Information System (APIS) – For screening purposes, APIS receives passenger and crew biographic data from commercial air and sea carriers prior to their arrival or departure from the United States.
U.S. Border Patrol Enforcement Operations System	
Enforce 3 (e3)	Implemented in 2008, Border Patrol agents use the e3 system to collect and transmit biographic and biometric data to identify each subject encountered during border security operations. The e3 system leads Border Patrol agents through a series of modules, including Processing, Biometrics, and Prosecutions. These modules support the agents during the various workflow stages of their daily intelligence-tracking, apprehension, and enforcement activities.
AMO Surveillance System	
Air and Marine Operations Surveillance System (AMOSS)	AMOSS is a radar surveillance system used to integrate air, land, and sea resources to detect, interdict, and prevent acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward or across the border.

Source: OIG-generated based on data provided by CBP

It is critical that OIT maintain adequate IT systems and infrastructure to fully support CBP's day-to-day, front-line border security operations. However, our 2012 audit report on CBP's IT management disclosed that CBP's Chief Information Officer (CIO) could not ensure that the component's IT environment fully supported mission needs.[4] We reported that systems availability challenges existed, including periodic outages of critical security systems, due in part to an aging IT infrastructure. We also concluded that the interoperability and functionality of CBP's IT systems needed improvement to effectively sustain CBP operations. As a result, CBP employees created workarounds or employed alternative solutions, including standalone, non-approved IT, to meet their needs. These practices hindered CBP from effectively accomplishing its mission and ensuring officer safety.

[4] *CBP Information Technology Management: Strengths and Challenges*, OIG-12-95, June 2012.

Results of Audit

CBP's IT systems and infrastructure did not fully support its border security objective of preventing the entry of inadmissible aliens to the country. The slow performance of a critical pre-screening system greatly reduced Office of Field Operations officers' ability to identify any passengers who may pose concerns, including national security threats. Further, incoming passenger screening at U.S. international airports was hampered by frequent system outages that created passenger delays and public safety risks. The outages required that CBP officers rely upon backup systems that weakened the screening process, leading to officers potentially being unable to identify travelers that may be attempting to enter the United States with harmful intent.

IT systems and infrastructure also did not fully support Border Patrol and AMO border security activities between ports of entry. Poor systems performance and network instability hampered these CBP operations nationwide. This resulted in excessive processing backlogs and agents' inability to meet court deadlines for submitting potential alien criminal prosecution cases. Also, frequent network outages hindered air and marine surveillance operations, greatly reducing the situational awareness needed to detect inadmissible aliens and cargo approaching U.S. borders. CBP has not yet addressed these long-standing IT systems and infrastructure challenges, due in part to ongoing budget constraints.

IT Infrastructure Did Not Effectively Support Traveler Screening Operations

CBP's IT systems and infrastructure did not effectively support day-to-day border screening activities. OFO personnel conduct screening at various stages of a trip to determine the admissibility of foreign nationals. IT infrastructure challenges, however, impeded pre-screening, reducing OFO officers' ability to identify individuals prior to their arrival who may pose a threat to national security. Frequent outages and poorly performing systems increased passenger delays and public safety concerns at ports of entry. Also, outages hampered the screening of passengers upon their arrival, requiring that officers rely on backup systems. These backup systems weakened the screening process and could potentially lead to officers not being able to identify travelers that may be attempting to enter the United States with harmful intent.

Pre-Screening Operations Impeded by Ongoing IT Modernization Efforts

OFO officers struggled to pre-screen and review information on travelers prior to their arrival in the United States. OFO officers pre-screen travelers by using IT systems to conduct law enforcement queries and check passenger flight

manifests.[5] Yet, poor performance of a critical pre-screening system hindered the ability of officers to identify individuals who could pose concerns, including national security threats.

A primary IT system used for traveler pre-screening was hampered by technology modernization efforts ongoing within CBP. OFO officers use the TECS Portal to research and identify international travelers who may pose threats to the United States in high-risk areas such as criminal activity and links to terrorism. The TECS Portal facilitates access to information across systems both within and outside of DHS that share law enforcement data. One such external system is the Federal Bureau of Investigation's central crime-related database called the National Crime Information Center. Officers also conduct analyses of incoming travelers listed on flight manifests in order to flag those who may require additional screening or more targeted examinations upon arrival in the United States.

Nevertheless, TECS Portal users stated that the system's performance had greatly diminished over the past year as a result of ongoing efforts to modernize the underlying system architecture.[6] Starting in May 2015, OIT deployed an updated TECS Portal environment, known as the "Modernized TECS Portal." This modernization activity involved transition from the legacy TECS mainframe to a web-based server environment.[7] OIT allowed users the option to remain in the legacy environment until the legacy system was turned off in December 2016.

Users told us that within the legacy environment, system response times and ease of navigation allowed them to complete pre-screening checks fairly effectively. However, the legacy environment was outdated and no longer supportable; therefore, CBP had to undertake efforts to modernize. OFO officers we interviewed stated they experienced poor system performance after switching to the modernized environment. They recounted frequent periods of system latency or non-responsiveness while conducting pre-screening checks.[8] The sporadic system performance and slow processing speeds forced users to wait an unreasonable amount of time for simple query results or responses to routine commands. For example, according to one officer, it took up to 30 minutes per flight to perform research and analysis of passengers for high-volume flights, as compared to 5 minutes per flight in the legacy mainframe TECS Portal

[5] CBP's pre-screening process includes multiple systems and is done hours, days, and in many cases weeks in advance through the National Targeting Center. The TECS Portal is one of several systems used in this layered approach to pre-screening passengers.
[6] TECS has been undergoing modernization since 2008 because its infrastructure has become outdated and costly to support.
[7] A server is a computer dedicated to hosting one or more services to serve the needs of other computer users on the network.
[8] Latency is a measure of the time it takes for data to travel from a computer to a server and back again.

environment. These difficulties could be attributed to the new web-based TECS environment, which required more bandwidth at field locations, such as airports, that used the CBP network.

Further, slow system performance left officers with less time to conduct critical passenger analysis, called targeting. Officers within airport passenger analysis units conduct targeting to identify travelers that have not already been flagged by a lookout, but may be a security concern in a high-risk area such as terrorism, criminal misconduct, or inadmissibility, among others. One officer we interviewed at San Francisco International Airport estimated that officers used to spend about half of their time on targeting to identify high-risk passengers; however, there was substantially less time available for this critical analysis following the TECS Portal upgrade. OFO personnel across multiple locations widely agreed the TECS Portal upgrade had an adverse impact on daily operations. To illustrate, 33 of 99 OFO personnel we surveyed reported slowness of query results within TECS negatively impacted traveler screening operations.[9]

The TECS Modernization Program took several steps to address these challenges. For example, program officials conducted outreach to identify issues for corrective action and promote user adoption of the modernized portal. They also took steps to improve the processing speed of the new portal, addressing a significant issue related to system query capability that had worked slowly since deployment in September 2016. This was corrected in December 2016 by upgrading to a new enhanced database server, among other changes, to improve query response time.

Nonetheless, more remained to be done to meet user needs. Specifically, the TECS Modernization Program had not conducted a thorough assessment of customer feedback as needed to identify and address user concerns regarding the portal. According to program documentation, such an assessment was to be done as part of an operational test at the completion of overall TECS modernization. The modernization program was scheduled to achieve full operational capability by June 2017, after the completion of our fieldwork, and the operational test would be completed thereafter.

Frequent System Outages Hampered Screening Operations at Airports

Passenger screening at U.S. ports of entry was hindered by frequent system outages and slow performance. OFO officers rely on IT systems and applications to expedite high volumes of inspections and screening operations at airports each day. However, system challenges caused passenger delays and prompted

[9] As part of this audit, we issued a written questionnaire surveying CBP personnel at the locations we visited within Border Patrol, OFO, and AMO. We received a total of nearly 200 responses from across all 3 offices.

the need to use backup screening methods that did not provide the same level of assurance for vetting passengers prior to entry into the United States.

Passenger Screening Process at Airports

Upon arrival, all international air travelers and baggage entering the United States must undergo inspection by a CBP officer to ensure admissibility. For example, CBP officers must determine the nationality of each traveler and, if determined to be a foreign national, whether the individual meets the requirements for admission to the United States.[10] OFO officers use a two-step inspection procedure to screen each traveler upon arrival at one of the 241 U.S. international airports around the county. Table 2 outlines the two phases of the passenger screening process.

Table 2: CBP OFO Passenger Screening Process

Inspection	
Primary	Upon arrival, each international traveler must clear passport control, also referred to as primary inspection. A foreign national entering the United States is required to present a passport and valid visa issued by a U.S. Consular Official, unless an exception applies, such as the individual is eligible for the Visa Waiver Program, a lawful permanent resident of the United States (possessing a Green Card), or a citizen of Canada. OFO officers inspect these and other travel documents before the traveler is admitted into the United States. If the OFO officer determines that additional screening is needed for a variety of possible reasons, the traveler will be referred to secondary inspection.
Secondary	During secondary inspection, an OFO officer may run law enforcement queries to screen travelers for admissibility issues. On average, 5% of travelers are referred to secondary inspection. If the officer determines there are no admissibility issues, the individual is permitted to enter the country.

Source: OIG-generated based on CBP data

OFO officers rely on IT systems and applications to expedite high-volume screening operations at airports each day. Figure 2 provides pictures of the three applications used to conduct primary screening: TPAC, Automated Passport Control, and Global Entry.

[10] *The Immigration and Nationality Act*, enacted in 1952, outlines Federal immigration and naturalization requirements (Public Law 82–414, 66 Stat. 163).

Figure 2: Primary Screening Applications at Airports

Source: CBP's public website

Each of these systems resides on the modernized TECS platform and must remain fully operational at all times to support front-line OFO officers and agents in screening and vetting travelers prior to admission. TPAC is specifically required to be available at least 99.7 percent of the time. This metric highlights the importance of properly functioning technology systems to process more than 300,000 incoming international air passengers each day.

Screening System Outages and Slow Performance

Although the TPAC, Automated Passport Control, and Global Entry applications facilitated the large daily volume of passenger screening, they did not meet the requirement to remain fully operational 24/7 for front-line officers. All three passenger screening applications experienced outages and periods of slow performance that hindered officers' ability to effectively screen and process incoming travelers. To illustrate, nearly 100 outages, periods of latency, or degraded service were reported for these applications between June 2016 and March 2017, totaling approximately 277 hours. The reports included 73 incidents that impacted TPAC. Some periods of latency had significant adverse impact on the performance of TPAC, causing users to experience long delays between transactions. The reported outages and periods of degraded performance reflect a range of issues with the primary screening applications and do not necessarily reflect nationwide incidents. Table 3 lists these incidents.

Table 3: Outages and Degradations Reported by OIT (June 2016 to March 2017)

	Total Number of Reported Issues	Total Hours Affected
June 2016	15	55.4
July 2016	14	20.0
August 2016	12	26.6
September 2016	2	0.9
October 2016	7	10.2
November 2016	14	27.5
December 2016	10	23.5
January 2017	10	65.4
February 2017	9	25.8
March 2017	6	22.0
Total	**99**	**277.3**

Source: OIG-generated based on data provided by the OIT

These service interruptions were prevalent during our audit fieldwork from December 2016 to March 2017. Two airports we visited experienced more than 82 hours of TPAC outages or degraded performance that adversely impacted screening of passengers on at least 715 flights. Specifically, OFO officials at Miami International Airport recounted approximately 78 hours of TPAC service interruptions between November 2016 and March 2017, which hindered screening of 91,850 passengers from 698 international flights. Similarly, OFO officials at Seattle-Tacoma International Airport recounted a TPAC outage of approximately 4 hours on March 27, 2017, which hindered screening of 3,391 passengers from 17 different flights.

OFO officers we interviewed expressed additional concerns regarding the frequency of TPAC interruptions, especially when they occurred during peak hours. Officers said that during periods of the latency, it could take several minutes for TPAC to return a query on an individual undergoing screening. Although some periods of latency did not warrant immediate action or concern, others prompted the need to seek resolution from OIT.

Poor Screening System Performance Attributed to Multiple Causes

OIT attributed these system outages and latency issues to multiple causes. Specifically, half of the reported incidents were due to maintenance and network infrastructure deficiencies. Such circumstances were typically resolved within a short period of time by OIT personnel. For example, the cause of a TPAC outage in late January 2017 was limited network capacity for certain field locations, which prohibited the successful transmission of data over the CBP network to

TPAC. To resolve this issue, OIT personnel switched circuits at the DHS data center in order to expand network capacity.

Further, approximately one-third of the TPAC incidents stemmed from dependencies on external systems that provided specific capabilities or services for screening within TPAC. In these cases, significant service interruptions prevented screening in TPAC as interfaces either failed or disrupted data transmission. For example, problems interfacing with IDENT frequently disrupted TPAC performance. These issues were resolved by technical support personnel within other DHS components responsible for the external systems.

According to OIT, another cause for a major TPAC outage pertained to ongoing modernization efforts that introduced changes to the TECS platform on which TPAC resides. Specifically, a significant TPAC outage occurred for 4 hours on January 2, 2017, caused by a change to APIS, which automatically feeds data to TPAC. The change was made to the underlying code logic in APIS that is used to validate travelers' information against carrier manifest information. OIT reported that the code change was introduced on December 28, 2016, when APIS transitioned to the web-based TECS platform as part of a TECS modernization deployment. This change caused the TPAC application to slow down to the point where it could not keep up with the high volume of passengers that needed to be screened during post-holiday travel. OIT ultimately transitioned APIS back to the legacy mainframe environment in order to restore service. The coding error was subsequently resolved in APIS.

OFO officers we interviewed at multiple airports identified additional instances of TPAC performance outages that were not reflected in the system's performance metrics. As such, TPAC outages were actually occurring more frequently than was apparent. OIT tracks system performance using metrics for availability, reliability, and other key indicators, and reports performance on a monthly basis to the DHS CIO. However, OIT's system availability metric did not include periods of slowness or service interruptions, such as interface failures, that occurred outside the TPAC system.

For example, the January 2, 2017 TPAC outage previously discussed was listed in OIT outage reports, but was not captured in the monthly performance report. Instead, OIT reported 100 percent TPAC availability for the month of January 2017. Despite the significance of the outage, OIT did not include the January 2, 2017 incident in its report, considering it an external APIS issue. This pattern was prevalent for a number of outages included in OIT incident reports from June 2016 to March 2017. Our comparison of these incident reports against monthly reporting on TPAC availability revealed discrepancies, ranging from –0.1% to –8.8%, in uptime reporting each month. For example, in March 2017 OIT reported 99.5 percent availability for TPAC; however, incident reports

indicated that the percentage of time with no reported issues impacting TPAC was 97.5 percent, or 2 percent less than the performance reflected in the metric.

Outages Resulted in Traveler Delays and Safety Issues

The system outages caused significant delays for travelers awaiting screening and entry to the United States. For example, the outage in January 2017 affected approximately 119,774 international travelers nationwide. About 13,000 passengers who arrived at Miami International Airport were faced with long lines and crowded conditions while awaiting screening. Figure 3 shows a photo of the frustrated passengers and overcrowded conditions during this incident.

Figure 3: Passenger Backlog at Miami International Airport January 2, 2017

Source: CBP staff at Miami International Airport

Such conditions also created hazards and security concerns. OFO officers we interviewed at Miami International Airport recounted numerous secondary challenges and risks, including difficulties with crowd control, temperature, health emergencies, and officer and public safety. CBP brought in additional support from Miami police and local fire departments to help mitigate these risks during this incident. Airport officials reported that 258 CBP officers worked 762 overtime hours, resulting in more than $58,000 overtime pay.

Backup Screening During Outages Was Not Fully Effective

Performance disruptions and outages resulted in the need to revert to backup systems to support screening procedures. The use of these procedures resulted in less effective screening practices that posed additional safety and national security risks.

CBP had standard operating procedures that outlined mitigation protocols to be followed during an unscheduled system outage or a significant system slowdown.[11] According to these procedures, a CBP port of entry Shift Supervisor would notify the Director of Field Operations, who has the authority to initiate mitigation protocols in the event that operations are adversely affected. Once initiated, OFO officers would begin to use the backup systems as appropriate to continue screening of incoming travelers during outages or severe degradations of service. Specifically, in the event that TPAC became unavailable, OFO officers would use the Automated Targeting System – Quick Query (ATS-QQ). If ATS-QQ or the CBP network became unavailable, OFO would use the Portable Automated Lookout System (PALS). Following is a description of each backup system for screening operations.

- ATS-QQ – This system requires access to a web-enabled computer and is the first alternative during an outage when network connectivity is uninterrupted. It provides limited query capability for law enforcement data. Data is current, back to the point when the TECS system became unavailable due to the outage, and includes full TECS and National Crime Information Center information.

- PALS – This is a standalone, laptop application for use during network outages, or when TECS and ATS-QQ are both down. The PALS application contains an extract of TECS law enforcement data and has the capability to run queries on this data. Each month, OIT updates PALS and distributes it via computer disk to all ports of entry.

As evident from these descriptions, the backup systems used during outages did not provide the same level of passenger screening as the standard systems. Instead, information used to vet passengers could be outdated, thereby increasing the risk that a traveler attempting to enter the United States with harmful intent could clear CBP inspection. Specifically, PALS lacked real-time law enforcement data because it was a standalone application to be used offline.

[11] CBP Directive 3340-041, *Standard Operating Procedures During System Outages at Air, Land, and Sea Ports of Entry*, November 26, 2007.

CBP officials stated the TECS data contained in PALS could be 2 to 6 weeks old, depending on when it was last updated.

Further, neither backup system included capabilities for conducting biometric checks during screening to confirm a traveler's identity. Specifically, because the PALS system was a standalone application and the ATS-QQ did not interface with IDENT, officers had to waive biometric checks entirely when TPAC went offline. Approval by the Director of Field Operations was required to cease the collection of biometrics during an outage. Without the use of biometric checks, OFO officers lacked the ability to identify any individual who might be traveling under an alias, or who might have a criminal record, thereby posing a national security risk.

OFO officers at multiple airports recounted numerous incidents when they relied on backup systems to process incoming travelers during recent outages. For example, officers at Miami International Airport cited 10 instances between November 2016 and March 2017 when system outages required mitigation, including the use of backup systems. Likewise, officers at Seattle-Tacoma International Airport reported using ATS-QQ during a 4-hour outage on March 27, 2017. Most concerning was the January 2, 2017 nationwide outage that caused 167 major airports to revert to mitigation procedures for 4 hours. During this outage, roughly 79 officers at Miami International Airport reportedly did not have access to ATS-QQ. These officers used PALS instead, which further compromised the screening process because they could not conduct biometric queries and relied on potentially outdated information.

Ongoing Initiatives to Improve Backup Screening Systems and Processes

During our fieldwork, OFO began several initiatives to improve backup capabilities for screening travelers. These initiatives were also intended to provide better information to ports of entry on when to begin and end backup processes in the event of an outage. Table 4 lists these planned improvements.

Table 4: Improvement Initiatives for Backup Systems and Processes

System or Application	OFO Improvement Initiative
TPAC	Dashboard – To provide port-level visibility on slowdown and outage status to assist management with mitigation decision-making.
ATS-QQ	Mobile Primary – To vet travelers, assign a class of admission and provide an electronically-generated I-94 form to record foreign national entry to the United States. This new application is intended to be the first mitigation strategy implemented during a TPAC outage.
PALS	PALS Next Gen – To provide more up-to-date data through on-demand TECS data extraction from a file server and transfer to ports of entry via a USB device.

Source: OIG-generated based on CBP data

These initiatives remained ongoing as of the end of our audit fieldwork in March 2017. The effectiveness of these initiatives cannot be determined until they are fully implemented.

Recommendations

We recommend that the Assistant Commissioner for OIT, in collaboration with the Office of Field Operations:

Recommendation 1: Conduct a user assessment of the TECS Portal to identify, evaluate, and address performance challenges in traveler pre-screening operations in the field.

Recommendation 2: Develop a plan to address maintenance, infrastructure, dependencies on external systems, and other factors that contributed to challenges regarding availability of primary traveler screening applications.

Recommendation 3: Assess the need for performance measures to monitor, evaluate, and ensure the availability of primary traveler screening applications from the end-user perspective at ports of entry.

Recommendation 4: Complete backup process improvement initiatives, including development of a dashboard for port-level visibility on system latency and outage status to assist management with mitigation decision making and upgrade of mitigation applications, as appropriate.

Poor System Performance and Network Instability Hampered Border Patrol and Enforcement Operations

IT systems and infrastructure critical to support Border Patrol and AMO operations between ports of entry were insufficient. Poor system performance and network instability hampered border enforcement activities nationwide.

These issues resulted in excessive processing backlogs and agents' inability to meet court deadlines for submitting potential alien criminal prosecution cases. Also, frequent network outages hindered air and marine surveillance operations, greatly reducing situational awareness needed to detect inadmissible aliens and cargo approaching U.S. borders. Long-standing challenges with obsolete IT infrastructure to support Border Patrol and AMO operations persisted, due in part to ongoing budget constraints.

Border Patrol Operations Constrained by System Outages and Poor Performance

The primary system used by Border Patrol agents, e3, did not effectively support mission operations. Border Patrol agents working in stations across all 20 sectors experienced periodic IT outages and slow performance, which hindered efficiency and, in some cases, prevented the timely transfer of information about criminal aliens for possible prosecution.

Border Apprehension and Enforcement Operations Depend on Technology

Border Patrol agents interdict and apprehend aliens along the border between ports of entry. Agents work around the clock to maintain traffic checkpoints, survey border areas, and conduct field patrol checks. One of the most important activities of a Border Patrol agent is field line watch. This involves the detection and apprehension of undocumented aliens and smugglers at or near a land border. In some cases, these operations involve capturing fairly large groups of illegal aliens, sometimes more than 140 subjects. During FY 2016, Border Patrol agents apprehended a total of 408,870 aliens along the southwest border.

The Border Patrol's day-to-day apprehension and enforcement activities rely heavily on technology. The primary system, e3, supports nearly 20,000 Border Patrol agents with critical capabilities to collect and share biometric data, including fingerprints, for identification and verification of individuals apprehended at the border. The e3 system consists of five modules (Intake, Processing, Biometrics, Detention, and Prosecution) that support each distinct action that a Border Patrol agent takes after apprehending a subject. The e3 system also serves as a web-based portal to share tracking and law enforcement activities daily with other DHS components.[12]

Agents rely on e3 around the clock, in three shifts, to input all alien apprehensions in the field. Specifically, for each subject apprehended, agents enter biographic and demographic data, take fingerprints, and perform biometric

[12] The e3 system connects to the Enforcement Integrated Database operated by U.S. Immigration and Customs Enforcement (ICE), and IDENT, the system deployed to capture biometric records as part of the former United States Visitor and Immigrant Status Indicator Technology program.

queries among various system interfaces such as IDENT. Once biometric results are returned, the agent determines the subject's disposition. Based on this disposition, an alien is subject to an appropriate immigration consequence, including potential criminal prosecution.

Border Apprehension and Enforcement Activities Were Hindered by Outages

Border Patrol agents were frequently unable to carry out border apprehension and enforcement activities due to outages and slow performance of the e3 portal or various e3 modules, each of which provides specific functionality. The most frequent outages related to the information sharing portal within e3, which shares real-time data with ICE's Enforcement Integrated Database. Some of these outages were prolonged. For example, four unplanned outages of the Enforcement Integrated Database occurred between July and October 2016; the most significant instance in July 2016 lasted for nearly 2 days.[13] Additional planned outages of this database occurred once a month for maintenance purposes. Table 5 provides examples of e3 availability and performance issues that occurred at a southwestern Border Patrol sector during 2016.

Table 5: Sample e3 Performance Issues at a Southwestern Border Patrol Sector May 2016 to October 2016

Date	Issue	Impact
May	e3 Processing experienced constant buffering.	Each alien file took about 4 hours to process, rather than the average 45 minutes. Although 12 hours was the target, subjects exceeded 24 hours in custody.
June	e3 biometric fingerprint queries took more than 2 hours to return results.	Delayed processing of apprehended aliens. Subjects remained in custody more than 24 hours.
July	e3 was unavailable throughout a multi-day Enforcement Integrated Database outage.	Inability to process or transfer subjects in custody. Some subjects were in custody more than 72 hours.
September	e3 was unavailable during an Enforcement Integrated Database outage.	Subjects in custody for more than 24 hours caused delayed transfer of unaccompanied alien children.
October	e3 biometric queries could not be performed.	Processing backlogs and extended time in custody.

Source: OIG-generated based on Border Patrol data

System slowness prevented Border Patrol agents from recording data on their enforcement operations in a timely manner. Such data needed to be quickly entered into the e3 system so that biometrics could be captured and used to identify apprehended aliens. The subjects' data also needed to be input to track custodial actions by Border Patrol agents, as well as track detainee movements

[13] In general, the Enforcement Integrated Database has been more stable outside of this period.

while in Border Patrol custody. However, the e3 system experienced regular periods of slow performance or lock-ups while processing transactions. According to Border Patrol agents, e3 often required complete system restarts after freezing. During our fieldwork, we observed system performance issues firsthand, including delays while logging in and system instability.

Border Patrol agents we surveyed indicated that the suite of e3 modules was generally unstable and slow. For example, one agent claimed that simply logging into the system and processing an apprehension was time consuming. Also, attempting to correct information within the system often resulted in additional errors that could significantly extend processing times. Another agent stated e3 was extremely unreliable and often crashed entirely after logging in. Multiple agents agreed that restarting the e3 system, or even restarting the computer entirely, was a common response to resolve system slowness. An internal user satisfaction survey conducted by the Border Patrol in the fall of 2016 corroborated that e3 performance was a significant concern. Although the overall rating in response to the survey was "average," numerous respondents rated e3 as below average or poor, stating that the system was extraordinarily slow on a daily basis. One respondent wrote that it took agents nearly double the amount of time it should to process nearly every individual they apprehended.

The frequent outages and latency stemmed from e3 interfaces with external systems and databases that provided specific services for each e3 module. Slow performance or disruptions to these interfaces resulted in an inability to perform certain functions or to use e3 entirely. For example, matching capabilities within the Biometrics Module were provided by external systems (e.g., IDENT), which sometimes experienced outages or planned maintenance that adversely affected e3 operations. Also, when the Biometrics Module was unavailable, e3 users could not capture and upload fingerprints or verify biometrics of the subjects apprehended. Border Patrol reported 18 biometric system outages between April 2016 and March 2017, ranging from 1 to more than 18 hours in duration.

Inability to Meet Criminal Prosecution Deadlines

The most significant impact of outages and slow processing in the e3 system was Border Patrol agents' inability to meet court deadlines for submitting information about criminal aliens for possible prosecution. Specifically, agents stated that when the online Prosecutions Module was unavailable, or when e3 service was disrupted, they could not timely prepare and electronically transmit criminal history records to the courts.[14] For example, to provide required

[14] Through a memorandum of understanding between DHS and the Department of Justice, CBP is required to upload data from the Prosecutions Module to a Justice website to facilitate criminal prosecutions and also provide material witness affidavits.

information for prosecution, Border Patrol agents had to input specific criminal charges, along with all information associated with the encounter, into the e3 Prosecutions Module. In general, these records were to be completed and transferred electronically to the appropriate U.S. district court within 48 hours of arrest.[15] Agents stated that U.S. district courts would often decline cases submitted just a few minutes late, preventing prosecution once a deadline had passed.

Border Patrol agents at multiple locations we visited stated that missing the deadline for transferring records for prosecution was not uncommon. In January 2015, for example, 48 individuals apprehended in the Tucson sector of the southwest border were not prosecuted due to late records submissions. Also, in April 2015, the same sector missed the deadline for transferring records for another 36 individuals due to e3 system failures. Agents in the Rio Grande Valley sector of the southwest border indicated they routinely missed deadlines for transferring required information for prosecutions due to e3 outages or the sheer volume of apprehensions.

The implications of missing deadlines for submitting information about criminal aliens for possible prosecution can be significant. Agents conceded that criminal prosecution of aliens is a fundamental component of border enforcement and is the most effective consequence for border violations to prevent recidivism. Prosecution of misdemeanor and felony acts is also central to deterring and preventing other criminal activities, such as alien smuggling and transport of illicit cargo. Officials lamented that when such deadlines are missed, CBP may only be able to pursue removal of aliens without pressing criminal charges.

Inability to Timely Process and Transfer Subjects

Border Patrol agents commonly acknowledged that system performance problems hindered their ability to keep up with the steady stream of high-volume apprehensions, especially along the southwest border. Specifically, thousands of aliens are apprehended daily, including large numbers of families and unaccompanied children. Poor e3 availability and slow performance hindered agents from timely completing data input on alien subjects following such field apprehensions. The time required to input biographic and demographic data into e3, conduct biometric queries, and transfer subjects for further disposition could quickly result in processing backlogs when large groups of aliens were apprehended.

[15] CBP advised that the U.S. district courts' deadlines for submission of information about criminal aliens for possible prosecution are a direct result of the 6th Amendment right of a defendant to a "Speedy Trial," and Rule 5 of the Federal Rules of Criminal Procedure. These deadlines varied by location as different U.S. district courts had different standards for prompt presentment based on that court location's interpretation of a defendant's Constitutional rights.

Agents at several Border Patrol stations explained backlogs in processing apprehended aliens resulted in a high number of subjects held in Border Patrol stations for prolonged time periods. Border Patrol had specific requirements for short-term custody of persons held at stations, checkpoints, or other processing facilities. Policy states that subjects normally should not be held for more than 12 hours as increased time in Border Patrol custody posed potential legal risks. Nevertheless, two stations we visited during our fieldwork reported holding subjects between 70 and 80 hours because of a lengthy system outage, far exceeding average time in custody. Other border stations and sectors reported similar concerns with protracted holding times caused by e3 issues.

To counter backlogs caused by e3 outages, Border Patrol reassigned patrol agents away from border security operations in the field to assist with alien processing and other administrative duties. For example, one station reported diverting eight agents from patrol duties to assist with clearing a processing backlog. In addition, some patrol agents were detailed full time to meet administrative alien processing requirements. The e3 system was designed to help Border Patrol agents keep up with alien processing. Diverting personnel from field operations to deal with processing backlogs defeated the purpose for which the system was designed.

More concerning, in one case, aliens were returned to Mexico with limited processing because of a prolonged e3 outage. Specifically, during the 2-day outage in July 2016, one sector along the southwest border reported that 10 unaccompanied Mexican national children were repatriated at the border crossing without first capturing their biometric data. Further, 27 adult Mexican nationals who had been identified using biometric data, but not yet processed for removal, were allowed to voluntarily return to Mexico without further processing.

System issues also created risks to Border Patrol agent safety. Specifically, if aliens could not be processed timely, holding facilities became overcrowded. One senior Border Patrol official said that during the July 2016 outage, the Rio Grande Valley Sector had an estimated 3,000 aliens in custody with holding space intended for only 1,800, creating an agent safety issue. Further, when agents were unable to conduct biometric checks on aliens, they might be unaware of whether they had dangerous individuals in custody and the need to take added precautions.

At the conclusion of our fieldwork, Border Patrol's Enforcement Systems Division had submitted an e3 modernization proposal to OIT. The proposal cited slow system performance, a lack of systems integration, external dependencies, and high costs to maintain outdated systems as justification for the requested

upgrades. Pending resolution of these issues, Border Patrol agents resorted to workarounds to document and track apprehensions. For example, agents at multiple locations we visited used Microsoft Excel spreadsheets to record the movement of subjects in their custody while e3 was unavailable. Such manual processing was error-prone, created data security vulnerabilities, and entailed added work as agents had to key the data into e3 once the system was restored.

Network Instability Obstructed Air and Marine Surveillance Operations

Critical surveillance technology did not reliably support AMO mission operations. Air and marine agents identify and deter inadmissible aliens and cargo approaching U.S. borders. Central to this mission is the Air and Marine Operations Center, which employs sophisticated technology for domain awareness and detection of air and sea border threats. The center uses live radar and surveillance capabilities to conduct real-time tracking of targets (i.e., aircraft and maritime vessels) and coordinate law enforcement response activities. The AMOSS is a primary surveillance system that the Air and Marine Operations Center uses 24/7 to maintain situational awareness.

Due to periodic network outages, AMO agents faced significant challenges using the AMOSS radar system to accomplish its mission. When fully operational, AMOSS can identify targets through 700 sensors and display 50,000 radar tracks at one time, making this system a crucial asset for multi-agency border surveillance operations. According to AMO Center officials, however, outages of the Redundant Trusted Internet Connection hindered AMOSS capabilities. The Redundant Trusted Internet Connection is a DHS-managed gateway that provides agency-wide Internet connectivity to the Department's network, DHS OneNet. DHS created OneNet in 2005 to consolidate component networks into an integrated technology infrastructure. Since the beginning of FY 2015, more than 25 separate network outages have disrupted AMOSS operations for a total of more than 350 hours, causing a loss of surveillance capabilities. AMO Center incident reports indicated that some outages lasted multiple days, although AMO officials noted that not all outages had equal operational impact.

AMO officials stated that these outages were a major concern, as any loss of surveillance capability increased the risk of undetected illegal border crossings or other dangerous criminal activity. Specifically, during these outage periods, the AMOSS lost input from key sensors that provided critical low-level radar coverage along the border. For example, the Tethered Aerostat Radar System is a key sensor system used to detect 45 percent of suspect tracks over the last 3 fiscal years. Network outage prohibited the transmission of data from this low-level radar system, creating a border coverage gap. During the most recent outage, on April 21, 2017, the AMOSS did not have input from the Tethered Aerostat Radar System and other critical sensors for 3.5 hours.

Long-standing Challenges with Obsolete IT Infrastructure Not Yet Addressed

CBP has not addressed long-standing deficiencies with its outdated IT infrastructure and equipment, which contributed to component-wide system performance and availability challenges. DHS policy states that component CIOs will timely deliver IT services in direct support of a component's mission, goals, objectives, and programs.[16] The Office of Management and Budget also instructs CIOs to rationalize their agency IT investments, such as enterprise IT systems, and key IT infrastructure services, including networks, desktop computers, and mobile devices, to ensure mission operations.[17] Based on these guidelines, CBP OIT was responsible for overseeing and directing how IT systems and infrastructure could best support mission operations. According to OIT documentation, however, significant infrastructure upgrades and modernization efforts were needed to improve the availability and performance of mission critical IT systems. The Assistant Commissioner of OIT identified modernization of CBP's aging IT infrastructure as one of three strategic priorities for FY 2017, because of its risk to CBP mission accomplishment.

Specifically, at the time of our audit, OIT reported that a considerable portion of IT equipment across the infrastructure had reached its end of life—defined as more than 5 years old. For example, 71 percent of the front-end infrastructure, including laptops and desktops, were obsolete. Also, OIT reported that 34 percent of the network infrastructure enabling connectivity and transfer of data across applications (e.g. switches), as well as 12 percent of the back-end infrastructure, including servers, were outdated.[18]

To illustrate, numerous field locations we visited used obsolete computers and other outdated IT equipment. This included laptops, workstations, card readers, fingerprinting devices, and tablets that were all approaching the end of their life cycle. Border Patrol agents at the Tucson sector reported that 87 percent of their computers were at least 5 years old. Similarly, agents at the Blaine sector stated that more than 120 of their computers and laptops were past their end-of-life dates with no replacement plans.

Further, field offices across CBP struggled with network bandwidth limitations. Numerous ports of entry, Border Patrol stations, and checkpoints all disclosed challenges related to limited network bandwidth. We obtained written reports from sectors we visited, outlining bandwidth challenges at numerous border patrol stations. For example, one station in the Tucson sector indicated that

[16] DHS Directive 142-02, *Information Technology Integration and Management,* February 6, 2014.
[17] OMB Memorandum 11-29, *Chief Information Officer Authorities,* August 8, 2011.
[18] A network switch is a device that helps connect machines on a network to one another and allows them to exchange, process, and respond to requests.

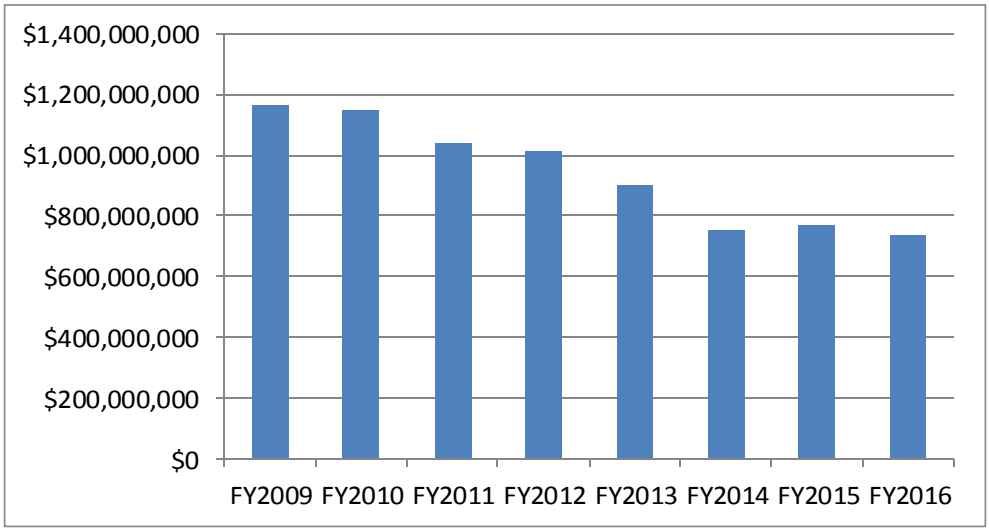
insufficient network capacity led to unacceptably slow system performance, as well as complete network outages. Another station reported that insufficient network connectivity resulted in safety concerns as officers relied on the network for tactical voice communications.

Results from our survey of CBP personnel further corroborated that system availability was a significant issue component-wide. To illustrate, 71 percent of the OFO personnel surveyed at the field locations we visited indicated that poor system availability impeded operations. Similarly, 68 percent of the Border Patrol agents at sectors and stations we visited reported the same issue. CBP personnel at numerous site locations we visited stated that network issues were exacerbated by an insufficient number of IT support personnel to help with immediate fixes at field locations.

Infrastructure Upgrades Not Completed Due to Budget Constraints

OIT was unable to ensure timely replacement of aging IT infrastructure because of ongoing financial resource constraints. Figure 4 shows OIT's declining budget from FY 2009 through FY 2016. According to OIT officials, in addition to a declining budget, OIT also faced increasing costs for operations and maintenance. For example, the cost of software licenses increased from 5 percent of OIT's budget to 23 percent during this time period.

Figure 4: OIT Top-Level Budget FY 2009 – FY 2016



Source: OIG-generated based on CBP OIT budget data

Problems with the outdated infrastructure have been a long-standing challenge. In June 2012, we reported that CBP's aging IT infrastructure was hindering

border security systems' availability.[19] We indicated that CBP personnel were working with obsolete hardware, such as computers and servers, as well as network components that had not been updated as needed.[20] For example, servers would typically be replaced every 3 years; however, CBP had a large number of servers that were being used beyond the recommended life cycle. Likewise, switches would typically be replaced every 5 to 6 years; however, at the time of our audit, some network switches were 12 to 14 years old. According to an estimate by a senior OIT official at that time, 70 percent of CBP's infrastructure was more than 4 years old.

OIT has taken significant steps since our 2012 audit to improve its IT infrastructure. According to officials, OIT continued to remediate CBP's highest vulnerabilities and upgrade end-of-life equipment as funding became available. OIT conducted an independent IT infrastructure assessment in FY 2012, which provided the basis for OIT to obtain funds to replace certain obsolete field equipment. About $22 million was allocated to upgrade CBP's most critical infrastructure needs, including servers, routers, and switches. In 2015, CBP also obtained funding for equipment upgrades to support cybersecurity initiatives, such as the Federal CIO's 30-day sprint to enhance the security and resilience of networks government-wide.

Nevertheless, more remains to be done to modernize CBP's IT infrastructure, as both our audit work and OIT's most recent assessments indicate. Until the needed upgrades are fully complete, Border Patrol and Air and Marine field agents will continue to struggle with systems availability and performance challenges that impede accomplishment of their critical border security mission operations.

Recommendations

We recommend that the Chief of the U.S. Border Patrol, in collaboration with the Assistant Commissioner for OIT:

Recommendation 5: Complete modernization plans for the e3 system to ensure adequate availability and functionality to support border security mission needs.

We recommend that the Executive Assistant Commissioner for Air and Marine Operations, in collaboration with the Assistant Commissioner for OIT:

[19] *CBP Information Technology Management: Strengths and Challenges* (Redacted), OIG-12-95, June 2012.
[20] Routers connect a network, acting as dispatchers to choose the best path for information to travel so it is received quickly.

Recommendation 6: Develop a plan to improve resolution time and mitigate the impact of network outages that degrade the capabilities of the Air and Marine Operations Surveillance System.

We recommend that the Assistant Commissioner for OIT:

Recommendation 7: Develop and implement a comprehensive technology refresh strategy and budget plan to upgrade outdated IT infrastructure and ensure adequate system availability and performance to support CBP's border security missions.

OIG Analysis of CBP Comments

We obtained written comments on a draft of this report from the Senior Component Accountable Official within CBP. We have included a copy of the comments in their entirety in appendix B.

In the comments, the Senior Component Accountable Official emphasized CBP's commitment to providing excellent IT support for border security operations. This official also noted that CBP uses a layered defense to vet travelers arriving in the United States which, along with backup systems, helps reduce risks regarding specific systems used for vetting and inspecting travelers at ports of entry. Further, the Senior Component Accountable Official stated that CBP takes the availability of border security systems very seriously and will leverage our report to help continue improving performance and availability of systems.

The Senior Component Accountable Official concurred with our recommendations and provided details on the actions that CBP is taking to address the specific findings and recommendations within the report. We reviewed the Senior Component Accountable Official's comments, as well as technical comments previously submitted under separate cover, and made changes to the report as appropriate. Following is our evaluation of the Senior Component Accountable Official's response to each of our report's seven recommendations.

Recommendation 1: We recommend that the Assistant Commissioner for OIT in collaboration with OFO conduct a user assessment of the TECS Portal to identify, evaluate, and address performance challenges in traveler pre-screening operations in the field.

Management Comments

The Senior Component Accountable Official concurred with recommendation 1 and stated that periodic user assessments are part of the TECS Modernization

program and provide valuable feedback to continually improve the system. OIT will conduct a user assessment focused on the TECS Portal as recommended. The estimated completion date for this action is December 31, 2017.

OIG Analysis

We agree that OIT's effort to complete a user assessment focused on the TECS Portal is a positive action toward addressing our recommendation. We look forward to receiving updates as this assessment is conducted and valuable feedback is provided to continually improve the system. This recommendation is open and resolved.

Recommendation 2: We recommend that the Assistant Commissioner for OIT, in collaboration with the OFO, develop a plan to address maintenance, infrastructure, dependencies on external systems, and other factors that contributed to challenges regarding availability of primary traveler screening applications.

Management Comments

The Senior Component Accountable Official concurred with recommendation 2 and stated OIT will develop a holistic plan for ensuring primary traveler system availability. The plan will include working with the external system owners to improve the availability of their services. The estimated completion date for these actions is December 31, 2017.

OIG Analysis

OIT's effort to develop a plan for improving availability of the primary traveler screening applications constitutes a positive step toward addressing this recommendation. We look forward to receiving updates as this plan is developed and implemented. This recommendation is open and resolved.

Recommendation 3: We recommend that the Assistant Commissioner for OIT, in collaboration with the OFO, assess the need for performance measures to monitor, evaluate, and ensure the availability of primary traveler screening applications from the end-user perspective at ports of entry.

Management Comments

The Senior Component Accountable Official concurred with recommendation 3 and stated OIT will work to increase monitoring of system response times. OIT also has implemented procedures to reach out to sites during system issues to

ensure that field impact is understood. The estimated completion date for these actions is December 31, 2017.

OIG Analysis

We agree that OIT's efforts to increase monitoring of transactions from end-users and implement procedures to notify sites during system issues are positive actions to address this recommendation. We look forward to receiving updates on implementation of these improved monitoring capabilities. This recommendation is open and resolved.

Recommendation 4: We recommend that the CBP Assistant Commissioner for OIT, in collaboration with the OFO, complete backup process improvement initiatives, including development of a dashboard for port-level visibility on system latency and outage status to assist management with mitigation decision making and upgrade of mitigation applications, as appropriate.

Management Comments

The Senior Component Accountable Official concurred with recommendation 4 and stated OIT and OFO are collaborating on how to better notify the field of system issues and clarify mitigation procedures. Additionally, they are deploying and upgrading backup systems to provide more up-to-date information when network connectivity is unavailable. The estimated completion date for these actions is December 31, 2017.

OIG Analysis

We agree with OIT's efforts to complete process improvement initiatives and upgrades to its backup application. We look forward to receiving updates on the implementation of these initiatives. This recommendation is open and resolved.

Recommendation 5: We recommend the Chief of the U.S. Border Patrol, in collaboration with the Assistant Commissioner for OIT, complete modernization plans for the e3 system to ensure adequate availability and functionality to support border security mission needs.

Management Comments

In responding to recommendation 5, the Senior Component Accountable Official concurred and indicated that e3 system modernization was in the planning stages, but funding would be required to support modernization efforts. Modernization is planned to begin in FY 2018, with implementation scheduled to occur incrementally between FY 2019 and FY 2023. CBP has established interim

milestones for incremental improvements to be made during FY 2018 to enhance the existing e3 system. The overall estimated completion date is September 30, 2018.

OIG Analysis

We agree with the actions described by the Senior Component Accountable Official to modernize the e3 system and establish independence from the Enforcement Integrated Database. We consider the planned interim enhancements to be an effective approach to enhancing system availability and functionality while CBP implements full modernization plans for FY 2019 and FY 2023. We look forward to receiving updates on these actions. This recommendation is open and resolved.

Recommendation 6: We recommend the Executive Assistant Commissioner for Air and Marine Operations, in collaboration with the Assistant Commissioner for OIT, develop a plan to improve resolution time and mitigate the impact of network outages that degrade the capabilities of the Air and Marine Operations Surveillance System.

Management Comments

In responding to recommendation 6, the Senior Component Accountable Official concurred and indicated that OIT will work with the DHS CIO to improve DHS OneNet network support of AMOSS. The OIT will also work to improve internal tracking and escalation of outages to OneNet for resolution. The estimated completion date is January 31, 2018.

OIG Analysis

We agree that the actions described by the Senior Component Accountable Official to resolve network support issues and improve outage tracking are positive steps toward addressing this recommendation. We look forward to receiving updates on the completion of these actions. This recommendation is open and resolved.

Recommendation 7: We recommend the Assistant Commissioner for the OIT develop and implement a comprehensive technology refresh strategy and budget plan to upgrade outdated IT infrastructure and ensure adequate system availability and performance to support CBP's border security missions.

Management Comments

The Senior Component Accountable Official concurred with recommendation 7 and indicated that OIT has developed a technology refresh cost analysis that will support an appropriate refresh cycle. The FY 2018 CBP budget includes requests for technology refresh funds, especially as they relate to the southern border. Future year funding of this initiative will depend upon DHS requirements and will reflect the priorities of the current Administration. The estimated completion date is November 30, 2017.

OIG Analysis

We agree with CBP's approach of developing a cost analysis to support technology refresh efforts. We understand that future year funding for the technology refresh will be dependent upon departmental requirements and the priorities of the current Administration. We look forward to receiving an update on actions taken for the FY 2018 refresh cycle. This recommendation is open and resolved.

Appendix A
Objective, Scope, and Methodology

The 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.

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of Departmental programs and operations, we conducted an audit to assess the effectiveness of IT systems to support the achievement of CBP's border security mission objectives of preventing the entry of illegal aliens or inadmissible individuals who may pose threats to national security.

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. We also 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 information-gathering meetings, documentation analysis, site visits, and system demonstrations to accomplish our audit objective.

We held meetings and teleconferences with CBP staff at headquarters and field locations. Collectively, we conducted more than 60 interviews, including meetings with headquarters officials and system users, to learn about CBP IT functions, processes, and capabilities. At headquarters, we met with the Acting Deputy Assistant Commissioner for the OIT and other OIT officials and representatives, as well as leadership, agents, officers, and support staff from OFO, Border Patrol, and AMO. We interviewed OIT officials, including Directors of OIT Directorates and system program managers, to discuss their roles and responsibilities related to CBP's border enforcement systems.

We visited field locations at West Palm Beach, Florida; Pembroke Pines, Florida; Miami, Florida; Homestead, Florida; Edinburg, Texas; McAllen, Texas; Rio Grande City, Texas; Pharr, Texas; Tucson, Arizona; Nogales, Arizona; Chula Vista, California; Riverside, California; San Diego, California; San Ysidro, California; Blaine, Washington; and Seattle, Washington; from January to March 2017. We also visited Miami International Airport, Seattle-Tacoma International Airport, Dulles International Airport, San Francisco International Airport, and the Air and Marine Operations Center located at Riverside, California. During these site visits, we met with directors, program managers, supervisors, Border Patrol and AMO agents, CBP officers, and system users, to

understand systems operation and performance, and infrastructure and support requirements. We discussed the existing IT environment, the extent to which it supported mission needs, and user involvement and communication with headquarters. We collected supporting documents about the CBP IT environment, systems, and technology-related improvement initiatives. We developed a questionnaire to obtain written input from officers and agents who use CBP's IT systems on a day-to-day basis. We obtained responses to the questionnaires from CBP personnel stationed at the field sites we visited. We analyzed their responses and reported on common trends across mission operations.

We conducted this performance audit between December 2016 and March 2017 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.

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

SEP 1 2 2017

U.S. Customs and Border Protection

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

FROM: Sean M. Mildrew
Senior Component Accountable Official
U.S. Customs and Border Protection

SUBJECT: Management's Response to OIG Draft Report:
"CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations" (Project No. 17-016-ITA-CBP)

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

CBP is committed to providing excellent information technology (IT) support for our border security operations. CBP utilizes a layered defense for vetting travelers arriving in the United States. This vetting begins when travel documents or authorizations are issued and continues as reservation data and advance passenger information is received from airlines prior to passengers boarding the plane. The advanced vetting includes extensive system checks of derogatory information and risk assessments. This vetting, along with CBP outreach to airlines and staff at major overseas airports, helps to ensure that travelers who pose a serious risk do not board the plane. Along with backup systems that can be used when passengers arrive in the United States, the advance vetting reduces the risk of the system issues noted in the subject report for vetting and inspecting travelers at our ports of entry.

CBP takes the availability of our border security systems very seriously and will leverage your report to help us continue to improve the performance and availability of our systems. Since a number of the identified issues in the report stemmed from dependencies on external service providers, CBP will continue to work with these providers to improve their services as well.

Most of the recommendations made in the report represent efforts that are already underway, and CBP will use them to continue to improve our technology support; therefore, CBP concurs with all seven recommendations in the draft report. Please see the attached for our detailed response to each of the recommendations.

Again, thank you for the opportunity to review and comment on this draft report. CBP's technical comments were provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Attachment

Attachment: Management Response to Recommendations Contained in OIG Draft Report: CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations (Project No. OIG-17-016)

The Office of Inspector General (OIG) recommended that U.S. Customs and Border Protection (CBP) Assistant Commissioner for the Office of Information and Technology (OIT), in collaboration with the Office of Field Operations:

Recommendation 1: Conduct a user assessment of the TECS Portal to identify, evaluate, and address performance challenges in traveler pre-screening operations in the field.

Response: Concur. Periodic user assessments are part of the TECS Modernization program and provide valuable feedback to continually improve the system. OIT will conduct a user assessment focused on the TECS Portal as recommended. Estimated Completion Date (ECD): December 31, 2017.

Recommendation 2: Develop a plan to address maintenance, infrastructure, dependencies on external systems, and other factors that contributed to challenges regarding availability of primary traveler screening applications.

Response: Concur. CBP's OIT has already been working actions to improve system availability for primary traveler screening applications. CBP's OIT will develop a holistic plan for primary traveler system availability that includes working with the external system owners to improve the availability of their services. ECD: December 31, 2017.

Recommendation 3: Assess the need for performance measures to monitor, evaluate, and ensure the availability of primary traveler screening applications from the end-user perspective at ports of entry.

Response: Concur. CBP has system monitoring tools that measure several internal transactions and a few transactions from end-user submission to end-user response times which help us assess the end-user experience. CBP's OIT will work to increase monitoring of transactions from end-user submission to end-user response times and has implemented procedures to call out to sites during system issues to ensure that the field impact is understood. ECD: December 31, 2017.

Recommendation 4: Complete backup process improvement initiatives, including development of a dashboard for port-level visibility on system latency and outage status to assist management with mitigation decision making and upgrade of mitigation applications, as appropriate.

Response: Concur. CBP's OIT and Office of Field Operations are collaborating on how to better notify the field of system issues and clarify mitigation procedures. The Automated Targeting System (ATS) Quick Query already provides a comprehensive TECS and National Crime Information Center (NCIC) check when network connectivity is available. Mobile Primary is also being deployed as a mitigation system. The Portable Automated Lookout System (PALS) is being upgraded so that it can be updated more frequently and facilitate the use of document readers when network connectivity is not available. ECD: December 31, 2017

Attachment to Management Response OIG Draft Report: "CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations" (Project No. 17-016-ITA-CBP)

The OIG recommended that the Chief of the U.S. Border Patrol, in collaboration with the Assistant Commissioner for the Office of Information and Technology:

Recommendation 5: Complete modernization plans for the e3 system to ensure adequate availability and functionality to support border security mission needs.

Response: Concur. The e3 system modernization is in the planning stages and will incorporate independence from the Enforcement Integrated Database (EID), while still providing data to the EID. Funding will be required to support e3 system modernization. U.S. Border Patrol (USBP) is undertaking a new business case to address the modernization of its Border Patrol Enforcement Systems (BPES), which includes the e3 application. This is a multi-year undertaking beginning in Fiscal Year (FY) 2018 with considerations of the overall planning effort to begin in FY 2019 and refactoring/development/implementation slated to occur between FY 2019 - FY 2023. In the interim, several incremental improvements to the e3 system will be made throughout FY 2018. Estimated interim milestones:

1. January 31, 2018: Develop Capability Analysis Report (CAR) to justify the requirement.
2. March 31, 2018: e3 enhancement release.
3. September 20, 2018: e3 enhancement release.
4. September 30, 2018: Complete preliminary modernization plan.

The overall ECD is September 30, 2018.

Recommendation 6: Develop a plan to improve resolution time and mitigate the impact of network outages that degrade the capabilities of the Air and Marine Operations Surveillance System.

Response: Concur. CBP's OIT will work with the Department of Homeland Security (DHS) Chief Information Officer (CIO) to improve the DHS OneNet network support for the Air and Marine Operations Surveillance System (AMOSS). CBP's OIT will also work to improve the internal tracking for outages and escalation to OneNet for resolution. Estimated interim milestones:

- October 31, 2017: CBP to meet with DHS CIO to request help in improving the OneNet support.
- January 31, 2018: Improve internal CBP processes that track outages and escalation to OneNet for resolution of the outage.

The overall ECD is January 31, 2018.

Recommendation 7: Develop and implement a comprehensive technology refresh strategy and budget plan to upgrade outdated IT infrastructure and ensure adequate system availability and performance to support CBP's border security missions.

Response: Concur. The CBP Office of Information and Technology (OIT) has developed a technology refresh cost analysis that will support an appropriate refresh cycle. The FY 2018 CBP budget requests technology refresh funds especially as they relate to the southern

Attachment to Management Response OIG Draft Report: "CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations" (Project No. 17-016-ITA-CBP)

border. Future year funding of this initiative will be dependent upon the requirements of the Department and will reflect the priorities of the administration. ECD: November 30, 2017.

Appendix C
Office of IT Audits Major Contributors to This Report

Kristen Bernard, Division Director
Steven Staats, Audit Manager
Christopher Browning, Auditor-in-Charge
Swati Nijhawan, Senior Program Analyst
Shawn Ward, Senior Program Analyst
Ann Brooks, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
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
Acting Commissioner, Customs and Border Protection
Customs and Border Protection Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305