OFFICE OF INSPECTOR GENERAL

CBP Has Improved Southwest Border Technology, but Significant Challenges Remain

Homeland Security

February 23, 2021

OIG-21-21

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

February 23, 2021

MEMORANDUM FOR: Troy A. Miller
Senior Official Performing the Duties of the Commissioner
U.S. Customs and Border Protection

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2021.02.22 15:16:43 -05'00'

SUBJECT: *CBP Has Improved Southwest Border Technology, but Significant Challenges Remain*

Attached for your action is our final report, *CBP Has Improved Southwest Border Technology, but Significant Challenges Remain*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving border security technology and situational awareness of the southwest border. Your office concurred with all three recommendations. Based on information provided in your response to the draft report, we consider all three recommendations resolved and open. 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. Please send your response or closure request to OIGAuditsFollowup@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 Thomas Kait, Acting Assistant Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG Highlights

CBP Has Improved Southwest Border Technology, but Significant Challenges Remain

February 23, 2021

Why We Did This Audit

Border security has been a mission priority since DHS' inception. Executive Order 13767, issued in 2017, directed DHS to strengthen southern border security. Technology is a critical component for gaining and maintaining operational control of the border. We conducted this audit to assess the effectiveness of CBP's current tools and technologies to support Border Patrol's mission to prevent the illegal entry of noncitizens who may pose threats to national security.

What We Recommend

We made three recommendations to improve technology and enhance situational awareness of the southwest border.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

In response to Executive Order 13767, U.S. Customs and Border Protection (CBP) has implemented an array of new tools and technologies that have enhanced Border Patrol's surveillance capabilities and efficiency along the southwest border. However, these upgrades are incomplete as CBP has deployed about 28 percent of the surveillance and subterranean technology solutions planned, even after receiving more than $700 million in funding since fiscal year 2017. Shifting priorities, construction delays, a lack of available technology solutions, and funding constraints hindered CBP's planned deployments. Consequently, most southwest Border Patrol sectors still rely predominantly on obsolete systems and infrastructure with limited capabilities.

CBP faced additional challenges that reduced the effectiveness of its existing technology. Border Patrol officials stated they had inadequate personnel to fully leverage surveillance technology or maintain current information technology systems and infrastructure on site. Further, we identified security vulnerabilities on some CBP servers and workstations not in compliance due to disagreement about the timeline for implementing DHS configuration management requirements.

CBP is not well-equipped to assess its technology effectiveness to respond to these deficiencies. CBP has been aware of this challenge since at least 2017 but lacks a standard process and accurate data to overcome it.

Overall, these deficiencies have limited CBP's ability to detect and prevent the illegal entry of noncitizens who may pose threats to national security. Deploying adequate technologies is essential for CBP to ensure complete operational control of the southern border.

CBP Response

CBP concurred with all three recommendations.

Table of Contents

Appendixes

Abbreviations

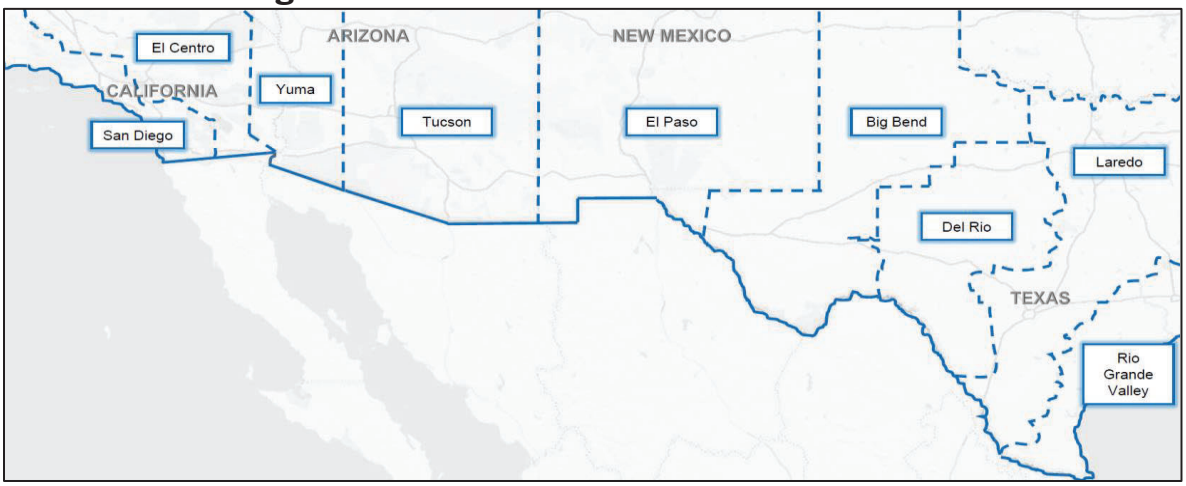
Border Patrol	U.S. Border Patrol
CBP	U.S. Customs and Border Protection
DISA	Defense Information Systems Agency
e3	Enforce 3
IAT	Information Assurance and Testing Branch
ICAD	Intelligent Computer Assisted Detection
IFT	Integrated Fixed Tower
IT	information technology
LGDS	Linear Ground Detection System
RVSS	Remote Video Surveillance System
STIGs	Security Technical Implementation Guides
sUAS	Small Unmanned Aerial Surveillance
TAK	Team Awareness Kit
TSM	Tracking, Sign-cutting, and Modeling

Background

Border security has been a mission priority since the Department of Homeland Security's inception. The southern border of the United States has long been vulnerable to cross-border illegal activity. Within DHS, U.S. Customs and Border Protection (CBP) is responsible for safeguarding America's borders from the entry of dangerous people and materials. Specifically, CBP's U.S. Border Patrol (Border Patrol) is charged with preventing people, terrorists, terrorist weapons, and contraband from entering the country between lawful ports of entry. Border Patrol's daily operations include detecting and tracking illegal entries, identifying and classifying those entries, responding to illegal activities, and resolving incidents through appropriate law enforcement actions.[1]

During fiscal year 2019, Border Patrol apprehended more than 859,000 people and seized more than 281,000 pounds of illegal drugs. The majority of these apprehensions (99 percent) and drug seizures (96 percent) occurred along the southwest border, which spans more than 1,900 miles between the United States and Mexico. In total, Border Patrol has more than 16,000 Border Patrol agents assigned to nine Border Patrol Sectors along the southwest border. These sectors are located in San Diego, California; El Centro, California; Yuma, Arizona; Tucson, Arizona; El Paso, Texas; Big Bend, Texas; Del Rio, Texas; Laredo, Texas; and Rio Grande Valley, Texas.[2] Figure 1 depicts Border Patrol's southwest border sectors and the operational boundaries.

Figure 1. Southwest Border Patrol Sectors



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

[1] *Border Security Improvement Plan*, Jan. 4, 2018
[2] The southwest Border Patrol sectors are divided into 47 stations, with agents assigned to patrol-defined geographic areas, or zones, within each station.

Federal Expectation for CBP to Strengthen the Southern Border Barrier

On January 25, 2017, the President issued Executive Order No. 13767, *Border Security and Immigration Enforcement Improvements* (Executive Order). The Executive Order directed the Secretary of Homeland Security to immediately plan, design, and construct a physical wall along the southern border, using appropriate materials and technology, to most effectively achieve complete operational control[3] of the southern border.

In response to the Executive Order, on February 20, 2017, then-Secretary John F. Kelly issued the memorandum, *Implementing the President's Border Security and Immigration Enforcement Improvements Policies*,[4] instructing CBP to immediately begin planning, designing, constructing, and maintaining a wall along the land border with Mexico in the most appropriate locations. In March 2017, CBP established a Wall Acquisition Program as a DHS "Level 1" major acquisition on the DHS Major Acquisition Oversight List.[5] Since fiscal year 2017, CBP has received nearly $7 billion in appropriations for procurements, construction, and improvements along the southern border. As part of this effort, the *U.S. Customs and Border Protection Strategy 2020–2025* outlines several initiatives aimed at improving border technology. These initiatives include using emerging technologies to promote situational awareness, rapid response capability, and agent safety, and establishing a resilient and secure information technology (IT) infrastructure to streamline operations.

Between fiscal years 2017 and 2020, CBP received more than $743 million in appropriations specifically targeted to fund the acquisition and deployment of technology to improve border security. Figure 2 shows the total annual appropriations for border security procurements, construction, and improvements, and the portion specifically appropriated for border security technology.

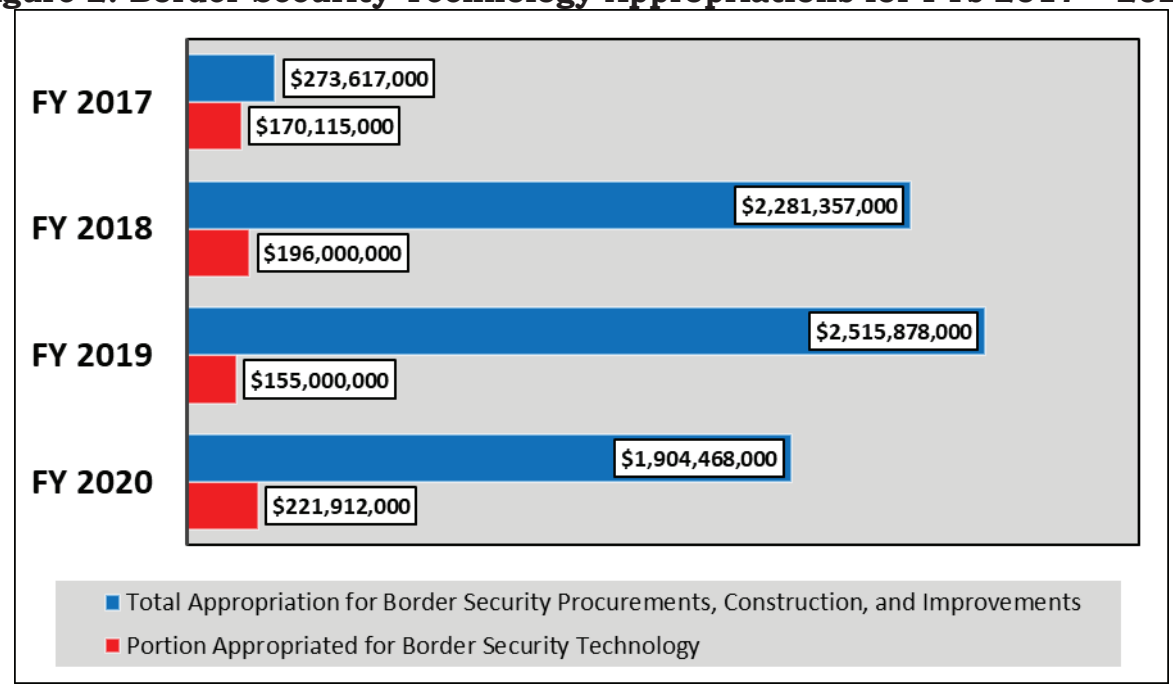
---

[3] Executive Order 13767 defines operational control as the prevention of all unlawful entries into the United States, including entries by terrorists and noncitizens, instruments of terrorism, narcotics, and other contraband.

[4] *Implementing the President's Border Security and Immigration Enforcement Improvement Policies*, Feb. 20, 2017, https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Implementing-the-Presidents-Border-Security-Immigration-Enforcement-Improvement-Policies.pdf

[5] The DHS Major Acquisition Oversight List identifies acquisition programs that are designated as Level 1 or Level 2 acquisitions, as well as portfolios, operational activities, and non-major programs, in accordance with DHS Acquisition Management Directive 102-01. Special interest programs or programs with life cycle cost estimates exceeding $1 billion, or service programs with an annual expenditure level exceeding $1 billion, are designated as Level 1 programs.

Figure 2. Border Security Technology Appropriations for FYs 2017 – 2020[6]



Source: DHS OIG analysis of Federal appropriations data

Importance of Technology for Border Security

According to DHS, the use of technology in the border environment is an invaluable force multiplier for increasing situational awareness. Technology supports persistent surveillance of large areas where individuals may attempt to cross illegally into the country or breach the border or border wall. CBP relies on various tools and technologies to support Border Patrol's mission operations in these challenging environments along the southwest border where agents face extreme conditions, such as steep mountainous terrain and dense ground cover. These conditions can impede physical access, make certain areas difficult for agents to patrol, and increase the need for effective technology. Figure 3 depicts the various southwest border environments.

[6] *Consolidated Appropriations Act, 2017*, Public Law 115-31, May 5, 2017; *Consolidated Appropriations Act, 2018*, Public Law 115-141, March 23, 2018; *Consolidated Appropriations Act, 2019*, Public Law 116-6, February 15, 2019; *Consolidated Appropriations Act 2020,* Public Law 116-93, December 20, 2019.

Figure 3. Southwest Border Environments
Source: DHS OIG photographs

CBP also uses a variety of independent and standalone surveillance systems and tools to enhance situational awareness and increase agents' capability to observe and respond to illegal activities along the border. Commonly used systems and tools include fixed and mobile surveillance equipment, agent-centric devices, unmanned aircraft, and sensor detection systems and devices.

Prior Audit Reports on CBP's Technology Challenges

CBP requires adequate IT systems and infrastructure to fully support Border Patrols' day-to-day, front-line border security operations. However, CBP has faced challenges maintaining up-to-date technologies, systems, and infrastructure to keep pace with ever increasing border security operations. Numerous audit reports during the past few years have highlighted concerns with CBP's ability to ensure its IT environment fully supports border security mission requirements.

- In 2017, we reported CBP's IT systems did not fully support border security operations, and its outdated IT infrastructure and equipment hindered field agents' ability to effectively complete required work.[7] In particular, a primary border enforcement application, Enforce 3 (e3), had system performance issues that prevented timely information sharing and processing of noncitizens.

- In 2019, we reported CBP did not have the IT system functionality needed to track separated migrant families during the execution of the *Zero Tolerance Policy*.[8] We found CBP had adopted various ad hoc methods to record and track family separations, which led to widespread errors and inefficiencies.

- In 2020, we reported Border Patrol did not use a sound methodology to identify and prioritize investments along the southwest border.[9] We found that without a comprehensive, well-documented approach, Border Patrol could not be certain it was making fully informed decisions about southwest border investments.

The Government Accountability Office (GAO) has drawn similar conclusions. In 2017, GAO reported Border Patrol made progress deploying certain technologies, but had not begun deployment of others.[10] Also, Border Patrol had not issued sufficient guidance to ensure accurate and reliable data on technology contributions, which limited its ability to determine mission benefits and inform resource allocation decisions.

We conducted this audit to assess the effectiveness of CBP's current tools and technologies to support Border Patrol's mission to prevent illegal entry of noncitizens who may pose threats to national security. This report documents the conditions based on data gathered during audit fieldwork from October 2019 through February 2020.

[7] *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations*, OIG-17-114, Sept. 28, 2017.
[8] *DHS Lacked Technology Needed to Successfully Account for Separated Migrant Families*, OIG-20-06, Nov. 25, 2019.
[9] *CBP Has Not Demonstrated Acquisition Capabilities Needed to Secure the Southern Border*, OIG-20-52, July 14, 2020.
[10] *Border Patrol Is Deploying Surveillance Technologies but Needs to Improve Data Quality and Assess Effectiveness*, GAO-18-119, Nov. 2017.

Results of Audit

In response to Executive Order 13767, CBP has implemented an array of new tools and technologies that have enhanced Border Patrol's surveillance capabilities and efficiency along the southwest border. But, these upgrades are incomplete as CBP has deployed about 28 percent of the surveillance and subterranean technology solutions planned, even after receiving more than $700 million in funding since FY 2017. Shifting priorities, construction delays, a lack of available technology solutions, and funding constraints hindered CBP's planned deployments. Consequently, most southwest Border Patrol sectors still rely predominantly on obsolete systems and infrastructure with limited capabilities.

CBP faced additional challenges that reduced the effectiveness of its existing technology. Border Patrol officials stated they had inadequate personnel to fully leverage surveillance technology or maintain current IT systems and infrastructure on site. Further, we identified security vulnerabilities on some CBP servers and workstations not in compliance due to disagreement about the timeline for implementing DHS configuration management requirements.

CBP is not well-equipped to assess its technology effectiveness to respond to these deficiencies. CBP has been aware of this challenge since at least 2017 but lacks a standard process and accurate data to overcome it.

Overall, these deficiencies have limited CBP's ability to detect and prevent the illegal entry of noncitizens who may pose threats to national security. Deploying adequate technologies is essential for CBP to ensure complete operational control of the southern border.

CBP Has Not Fully Deployed the Tools and Technologies Needed to Enhance Southwest Border Security

During the past 3 years, CBP has deployed new surveillance technologies, initiated system modernization efforts, and upgraded the IT infrastructure supporting its Border Patrol stations. These upgrades have enhanced Border Patrol's surveillance capabilities and efficiency. However, a number of CBP's planned technology deployments were incomplete at the time of our audit in February 2020 due to shifting priorities, construction delays, a lack of available technology solutions, and funding constraints. Consequently, most southwest Border Patrol sectors still rely on obsolete systems or technologies with limited capabilities to support mission needs.

Technology Improvements to Enhance Southwest Border Security

Since FY 2017, CBP has received more than $700 million to deploy new and modernized technology solutions along the southwest border. Notably, CBP deployed previously planned surveillance technologies, including fixed towers, remote surveillance systems, and mobile surveillance systems. Also, beginning in FY 2018, CBP introduced several new technology solutions, including innovative towers, aerial surveillance aircraft, and the team awareness application to enhance Border Patrol's surveillance capabilities. Table 1 describes each technology system, as well as completed deployments at southwest border locations.

Table 1. Key Border Technology Systems

	**Integrated Fixed Towers** (IFT) provide long-range, persistent surveillance of rural and remote areas. Each tower is equipped with sensors that continuously detect and track items of interest such as people crossing the border on foot or traveling in vehicles or low-flying aircraft, and provide that information to a Border Patrol command center. Between 2017 and February 2020, CBP deployed 31 IFT to the Tucson Border Patrol Sector.
	**Remote Video Surveillance Systems** (RVSS), provide persistent, wide-area surveillance and real-time video analytics of rural, urban, and remote areas. Each unit consists of color and infrared cameras mounted on fixed or relocatable towers, or on building structures, and remotely operated from Border Patrol stations. Between 2018 and February 2020, CBP deployed 41 RVSS along the southwest border.
	**Mobile Video Surveillance Systems** (MVSS) provide mobile response capability enabling Border Patrol to respond to changes in risk along the border. Each unit consists of a vehicle, a telescoping mast, and a technology suite with infrared and video sensors, a laser range finder, and a laser illuminator controlled by an operator within the vehicle. Between 2018 and February 2020, CBP deployed 58 MVSS along the southwest border.

	**Innovative Towers** provide nearly-autonomous capability to identify and classify items of interest without the direct control of a human operator. Equipped with artificial intelligence, this asset discerns between humans and other things, and alerts agents only to human activity. Between 2019 and February 2020, CBP deployed 46 innovative towers along the southwest border.
	**Small Unmanned Aerial Surveillance** (sUAS) is remotely-operated aircraft, weighing 55 pounds or less, capable of covert aerial surveillance and supporting search and rescue operations in remote areas with challenging terrain. Between 2019 and February 2020, CBP deployed more than 100 sUAS units along the southwest border.
	**Team Awareness Kit** (TAK) is a smart phone application that provides agents with communication and data sharing capabilities, and the ability to see team member locations in the field, reduce friendly fire incidents, and help coordinate movements. Between 2018 and February 2020, CBP deployed TAK-enabled phones to more than 5,900 agents in 4 southwest Border Patrol sectors.

Source: DHS OIG analysis of CBP-provided data

According to Border Patrol officials we interviewed, the introduction of these new and innovative technologies has improved operations and situational awareness along the southwest border. Senior field agents said that remote video surveillance had doubled their operational capability by providing visibility in low-coverage areas, and added much-needed situational awareness of noncitizen travel patterns and persons carrying weapons. According to senior agents we interviewed, modern solutions like innovative towers and sUAS have further enhanced Border Patrol's capabilities. Innovative towers provide alerts directly to field agents, instead of to the Border Patrol command center, which enables quicker field response. Border Patrol uses sUAS aircraft to conduct aerial surveillance of ground activities, and map areas that are difficult for agents to access by vehicle or on foot patrol. A Tucson Sector official said that sUAS was used to aid in searching for noncitizens who had gotten lost in the Arizona desert.

CBP also initiated modernization efforts to improve its most critical border security technology systems. In FY 2019, Border Patrol began a multi-year effort to modernize its suite of enforcement IT systems, which includes e3; Tracking, Sign-cutting, and Modeling (TSM); and Intelligent Computer Assisted Detection (ICAD).

Collectively, field agents use these applications to detect, deter, identify, and resolve illegal border activities, while also managing Border Patrol's resources. Following modernization, Border Patrol expects that these systems will provide improved data integration and information sharing and a more consistent and efficient workflow for agents and leadership. Table 2 lists Border Patrol's enforcement systems.

Table 2. Border Patrol's Enforcement Systems

System	Description
Border Patrol Enterprise Reporting Tool	Displays enterprise-level data for Border Patrol to create reports that inform operations and document enforcement statistics.
Border Patrol Enterprise Tracking System	Used by Border Patrol to schedule and track operations, manpower allocation, and asset deployments.
Enforce, 3rd Generation	Used by Border Patrol agents and others to process arrests and seizures in a workflow with various modules for processing detainees, detention tracking (cell movements/custodial actions), court prosecutions, biometric capture and searching, and other functions.
Enterprise Geospatial Information Services	Visually depicts border resources and activities, and provides the capability to view and analyze illicit activities and resource deployments over time and space.
Intelligent Computer Assisted Detection	Used by Border Patrol as its primary system for tracking agent dispatch and officer safety, and for real-time monitoring of unattended ground sensors and other surveillance resources during operations.
Operational Requirements Based Budget Program	Uses data from Border Patrol sectors to provide allocation-based spend plans; enables sectors to specify capability gaps and resources needs.
Tracking, Sign-Cutting, and Modeling	Provides near real-time spatial representation of agent activity, sign-cutting, and tracking operations in the field.

Source: DHS OIG-generated using Border Patrol-provided data

CBP has also completed much-needed upgrades to its field IT infrastructure and equipment. Since FY 2017, along the southwest border, CBP's Office of Information and Technology (OIT)[11] has upgraded 53 network routers and 409 network switches, and replaced more than 10,000 desktop computers, 2,000

[11] OIT manages CBP's technology and IT infrastructure to enable mission readiness and improve the ability of all employees, including field agents, to proactively respond to new threats.

laptop computers, and 900 tablet devices. These upgrades have improved the efficiency of field agents' work and have increased network speeds and capacity at numerous locations. CBP has plans and funding set aside to continue updating its IT infrastructure and equipment at other southwest border facilities.

Delayed Technology Deployments on the Southwest Border

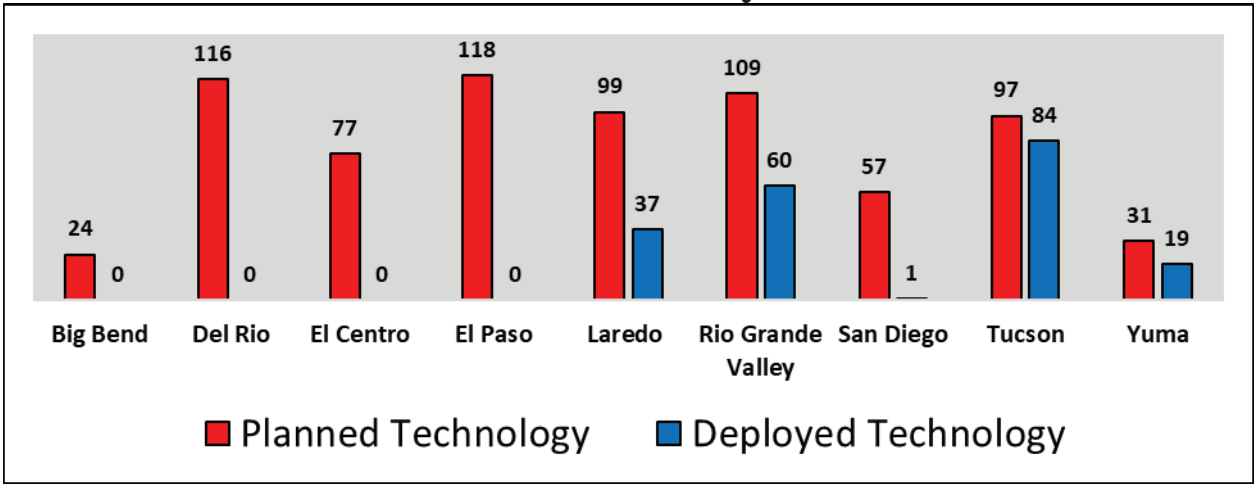
Executive Order 13767 directed CBP to construct a physical wall and use appropriate technology to achieve complete operational control of the southern border. However, CBP's technology deployments to the southwest border continue to be delayed, despite receiving technology-specific funding increases since FY 2017. Specifically, planned deployments of surveillance systems, infrastructure upgrades, and subterranean technology solutions were incomplete or behind schedule due to border wall construction delays, challenges identifying subterranean technology solutions, funding constraints, and shifting operational priorities.

Shifting Priorities Impacted Surveillance Systems Deployment

In accordance with its 2014 *Southwest Border Technology Plan*,[12] CBP planned to deploy a significant number of surveillance systems to Border Patrol sectors responsible for securing the southwest border. However, Border Patrol has only been able to deploy about 28 percent of the surveillance technologies planned for its southwest border sectors. To illustrate, as of September 2019, the Rio Grande City Border Patrol Station in Texas received only 9 of the 18 RVSS camera towers planned for installation. As of February 2020, approximately 72 percent (at least 527 of the 728) major surveillance systems listed in the 2014 plan had not been deployed, leaving many border areas more vulnerable to illegal activities. Figure 4 shows the number of planned systems versus the number deployed for each southwest border sector.

[12] Published in June 2014, CBP's *Southwest Border Technology Plan* incorporated previous southwest border technology plans, and captured the Secure Border Initiative Network Analysis of Alternatives, follow-on operational assessments, Border Patrol sector technology location plans, and associated cost estimates.

Figure 4. Total IFT, RVSS, and MVSS Planned vs. Deployed June 2014 – February 2020



Source: DHS OIG analysis of CBP-provided data

Surveillance technologies were deployed to specific locations based on mission needs outlined in the 2014 *Southwest Border Technology Plan*. However, CBP's technology priorities have changed since the 2014 plan, given the introduction of more innovative solutions, changing field needs, and evolving threats. For example, CBP adjusted its technology funding allocations to support new solutions like TAK and sUAS, which slowed or delayed all planned technology deployments. In FY 2018, $3 million was allocated for the initial deployment of TAK-enabled mobile devices — a high-level component priority. However, a senior program official said that TAK was, and remains, an unfunded budget requirement, for which Border Patrol had to divert funding from other technology programs to support CBP's expectation of continued TAK deployments and system support. Additionally, in FY 2019, CBP realigned $2.85 million in Mobile Surveillance Capability Program funding to training and technology support for the sUAS program. More recently, CBP requested $385 million for IFT program deployments that were part of the *Southwest Border Technology Plan*. However, that funding was not approved, which further delayed IFT deployments, now projected for FY 2021.

Subterranean Technology Delayed by Border Wall Construction Challenges

To meet the need for domain awareness,[13] CBP recently began introducing subterranean technology solutions to monitor traffic along the border wall and address the growing threat of cross-border tunneling. Border wall technology will include a new Linear Ground Detection System (LGDS). The key elements

[13] *U.S. Customs and Border Protection Mission Need Statement for Domain Awareness – Land Surveillance*, Nov. 1, 2018.

of LGDS are the detection sensor cable, power sources, supporting communications, and the user interface that displays alerts at the local Border Patrol station. CBP expects these technologies will promote detection of illegal activities such as persons climbing the wall or digging nearby. For the near-term, CBP planned to deploy approximately 40 linear miles of LGDS technology by the end of FY 2018. For the long-term, CBP plans to deploy more than 1,100 miles of LGDS along the southwest border by FY 2027.

However, CBP did not meet its plan to deploy 40 miles of LGDS technology by the end of FY 2018. As of February 2020, only about 12 miles of LGDS equipment had been installed along the border wall. Figure 5 shows newly constructed border wall sections in California and Texas where LGDS will be installed.

Figure 5. Border Wall Sections Recently Constructed in California and Texas

Source: DHS OIG and Border Patrol photographs

The delays in physical installation of LGDS system equipment were primarily attributed to ongoing disruptions to border wall construction. According to Border Patrol, in an effort to save time and money, CBP aligned the physical installation of the LGDS system equipment with border wall construction. Meaning, as the contractor constructed the wall, it also physically installed the LGDS sensor cable and supporting equipment. However, border wall construction experienced frequent delays due to issues such as extended real estate negotiations and amendments to construction designs, which slowed LGDS installation. Also, border wall construction was planned in segments, with each segment constituting a different project for which land had to be procured or otherwise obtained by CBP. The land for each wall segment project is often privately owned, possibly by multiple parties, all of whom must approve

of CBP's use of the land for wall construction. If approval from all land owners cannot be obtained, the land cannot be used and wall construction designs must be amended. Some land areas are protected by law, which restricts the land's use. For example, at the Rio Grande Valley Sector, a wall construction design was amended to account for a wildlife conservation area located on restricted-use land. Ultimately, once the physical installation of LGDS equipment is completed, Border Patrol must negotiate a separate contract to activate LGDS technology and connect it with station command centers for operational use.

Tunnel Detection Solution Delayed by Lack of Available Technology

Since 1990, Border Patrol has discovered approximately 190 cross-border tunnels through manual methods such as human observation of traffic patterns, law enforcement efforts, and routine patrol operations. Figure 6 shows: a) a sophisticated tunnel with lighting and ventilation; b) a rudimentary tunnel under the southwest border; and c) a clandestine tunnel that connects buildings in the United States and Mexico.

Figure 6. Examples of Cross-border Tunnels
Source: CBP

Border Patrol expects that security improvements introduced by the new border wall may increase the threat of cross-border tunneling. But, CBP currently lacks adequate technology to detect tunnels or tunneling activities, or monitor permanent, cross-border tunnels. Senior Border Patrol officials expressed during interviews an urgent need for a technology solution to aid detection efforts and alleviate risks to field agents. For example, the San Diego Sector has 36 storm drain tunnels that require 24/7 monitoring by patrol agents. These storm drain tunnels must often remain open to allow for normal operations and, absent technology capability, require direct physical surveillance to deter illegal access. Figure 7 shows cross-border tunnels that require persistent surveillance to prevent illegal crossings and other illicit activities.

Figure 7. Examples of Tunnels Crossing the United States/Mexico Border
Source: DHS OIG photographs

In September 2012, CBP established the formal operational need for tunnel detection technology,[14] but remained unable to implement an effective solution for field use. Nearly 7 years later, in January 2020, DHS approved the Cross-Border Tunnel Threat program, which Border Patrol described as a network of permanently-installed sensors to detect, classify, and localize subterranean activities. According to Border Patrol, the sensors will provide enhanced surveillance in areas where other technologies are hindered by terrain, foliage, or sustainability issues such as harsh climate conditions.

In FY 2020, CBP planned to implement 6 miles of Cross-Border Tunnel Threat capability along the southwest border, with nearly 100 total miles planned for deployment by FY 2030. However, as of February 2020, CBP had not yet implemented this technology for use during border security operations. According to Border Patrol officials, establishing an effective solution for tunnel detection required many years of development because technology with the unique requirements involved in detecting tunnels did not exist.

Since 2012, CBP has devoted extensive time and effort to defining operational requirements, conducting market research and technology demonstrations, and completing an Analysis of Alternatives[15] to determine the best available technology capability for detecting the various types of tunnel activities encountered along the southwest border. According to a senior program official, until recently, the tunnel detection capabilities that existed on the market were technically immature and did not meet CBP's mission

[14] *Mission Need Statement for Cross-Border Tunnel Threat Operations*, Sept. 21, 2012.
[15] An Analysis of Alternatives is an analytic decision-making process to identify and document the optimal solution for satisfying an identified mission capability gap.

requirements. The official also said this type of technology had little commercial demand and was not widely available, which contributed to the slow development process. Program management staff said that it has taken years to mature a technology; now it must be adapted to CBP's needs to ensure it is operationally sufficient.

CBP Has Not Addressed Aging Infrastructure and Obsolete Technology

Border Patrol personnel are further hindered by an inability to easily share operational information across non-integrated border technologies and sensors. Nearly every surveillance technology platform and enforcement IT application used in border operations was developed individually as a stand-alone system. For example, stand-alone field technologies such as IFT and RVSS were developed separately, many years ago, and are unable to interact or share information. As a result, personnel at Border Patrol command centers operate and monitor IFT and RVSS cameras separately. Similarly, adjacent Border Patrol stations lack the ability to share technology feeds during operations. For example, if an IFT is tracking a noncitizen, smuggling, or trafficking group traveling between station boundaries, no capability exists to share live video footage, or transfer control of the technology, across the stations. Instead, tracking is done by voice communication between stations and field agents using a mobile radio system.

Additionally, many Border Patrol sectors continued to struggle with limited bandwidth and slow network speeds, which degraded field agents' ability to access and process information. Officials from one sector said that every station in their area had limited bandwidth, which routinely impeded technology operations, such as tower-based surveillance cameras. Moreover, limited bandwidth continued to impede technology performance at Border Patrol's checkpoints along interstates and highways. For instance, CBP's License Plate Reader program alerts checkpoints of incidents involving vehicles. However, limited bandwidth at checkpoint stations slowed information relay, and Border Patrol missed stolen vehicles that passed through checkpoints before on-site agents received alert notifications.

More concerning, much of Border Patrol's existing field technology has exceeded its useful life and has suffered from degraded performance and supportability. For example, RVSS video systems have been used extensively for many years to provide persistent video surveillance across each Border Patrol station's operating area. However, many of these systems range from 15 to 20 years old and suffer from frequent malfunctions or repair issues. Replacement parts are obsolete and these systems are no longer supported by the manufacturer. While visiting a Border Patrol command center in

California, we observed an RVSS video monitor screen that was out of service. The supervisor said that the camera providing the video feed to that monitor had been out of service for approximately 3 months while awaiting repair, which had degraded the situational awareness of the area normally covered by that camera tower. In another instance, a sector official from Texas said an RVSS camera had been out of service for more than 15 months due to obsolete repair parts. The sector had to establish a contract with a third-party vendor to repair the camera by manufacturing obsolete parts that were no longer available for purchase.

Similarly, some of CBP's field infrastructure had surpassed its expected service life, but was still in use for day-to-day operations. For example, 18 towers used to support Border Patrol's surveillance technology and radio communications system had deteriorated to a condition considered unsafe for technicians to climb to perform maintenance and repair work. Used daily in sometimes harsh weather conditions, some of these towers had been in service for more than 20 years. Likewise, the Intelligent Computer-Assisted Detection application is nearly 20 years old, while e3 is 12 years old.

Technology Upgrades Were Stalled by Inadequate Funding

Although CBP has received more than $1.7 billion to fund technology since instituting its 2014 *Southwest Border Technology Plan*, funding constraints have limited full-scale deployment of much-needed technologies to the southwest border. Even the targeted technology funding received since FY 2017 has not been adequate to fulfill all requirements. A senior technology program official said that Border Patrol has been hundreds of millions of dollars short in fulfilling field technology requirements.

CBP also does not have adequate funds to modernize and integrate systems. In line with its current strategic goals[16] of improving data integration and establishing a common operating picture,[17] Border Patrol's technology program office planned to establish a capability that integrates disparate technology sensor feeds into an overarching common operating picture of the field environment. This is intended to facilitate information sharing between field agents and CBP headquarters offices. However, program officials said that funds for this effort will not be fully available until FY 2022.

[16] *U.S. Customs and Border Protection Strategy 2020 – 2025.*
[17] A common operating picture is a situational awareness capability that supports DHS' mission by sharing information to facilitate collaborative planning and response to threats.

Technology Effectiveness Is Further Hampered by Limited Manpower and Security Vulnerabilities

Border Patrol faced additional impediments that reduced the effectiveness of its technology on mission operations. Specifically, Border Patrol officials stated they lacked the manpower to fully utilize field technology systems for surveillance as CBP continued to struggle to fill gaps created by routine staff retirements and resignations. CBP also stated it lacked on-site support personnel to maintain its increasingly complex technology and infrastructure. Further, we identified security vulnerabilities on some CBP servers and workstations that were not in compliance with DHS configuration management requirements.

Technology Is Frequently Underutilized or Unavailable

Field technology systems such as ground sensors, imaging sensors, and tower-based cameras provide persistent surveillance in remote areas along the border. When items of interest are detected, the systems transmit alerts—motion, video, or photograph—to Border Patrol command center workstations. Border Patrol agents at command centers forward the alert information to field agents on patrol duty. These alerts are critical, as they are intended to indicate possible illegal activity.

However, these field technology systems were frequently underutilized during day-to-day operations. Numerous Border Patrol officials we interviewed claimed that agents were often unable to respond to surveillance technology alerts because they were assigned to other duties unrelated to physically patrolling the border. These duties included processing detainees, transporting detainees for medical treatment, operating vehicle checkpoints, and staffing station command centers. For example, during the 2019 surge in families crossing the border, a supervisory agent we interviewed said more than 60 percent of the agent workforce at the McAllen Station in Texas was used full-time to process and manage persons being held at the station. During that same time, technology systems continued generating alerts of field activities, but agents were unavailable to respond.

In addition, personnel at many Border Patrol sectors and stations said they lacked adequate staff to operate technology and respond to technology alerts. As of September 2019, Border Patrol was staffed with more than 21,000 employees, including uniformed agents and operational support staff. Southwest border sectors accounted for more than 18,000 of those personnel,

of which more than 16,700 were Border Patrol agents. However, senior field officials said the number of agents on staff was not enough to effectively complete required work.

Table 3 shows the number of Border Patrol agent positions authorized for southwest Border Patrol sectors, the number of agents assigned to those positions as of February 2020, and the number of positions unfilled.

Table 3. Southwest Border Patrol Staffing as of February 2020

Border Patrol Sector	Agent Positions Authorized	Number of Agents Assigned	Number of Unfilled Positions
Big Bend	640	532	-108
Del Rio	1,641	1,504	-137
El Centro	1,121	859	-262
El Paso	2,415	2,172	-243
Laredo	1,851	1,763	-88
Rio Grande Valley	3,199	3,119	-80
San Diego	2,484	2,251	-233
Tucson	3,825	3,658	-167
Yuma	810	804	-6
	17,986	**16,662**	**-1,324**

Source: DHS OIG-generated using of CBP-provided data

Executive Order 13767 directed CBP to hire 5,000 additional Border Patrol agents and take all appropriate action to ensure the new agents entered on duty as soon as practicable. However, as of March 2020, CBP had not yet hired any additional agents, as it struggled to fill ongoing gaps created by routine staff retirements and resignations. In November 2019, we reported that, although directed to do so by Congress in 2011, CBP had not completed a satisfactory workforce staffing model.[18] As of March 2020, Border Patrol had developed a draft staffing model, which was under review by DHS, but it had not yet been implemented or used to inform staffing decisions. Also, according to a workforce management official, CBP had not received funding to hire any of the 5,000 new agents authorized by Executive Order 13767.

Border Patrol also lacked adequate on-site support personnel to maintain its increasingly complex technology and infrastructure and ensure its availability for operational use. CBP's OIT maintains many field technology systems and repairs malfunctioning systems, while the Office of Facilities and Asset

[18] *Major Management and Performance Challenges Facing the Department of Homeland Security*, OIG-20-02, Nov. 13, 2019.

Management maintains technology infrastructure, including towers and power supplies, access roads, and the fencing needed to protect assets from unauthorized access. However, these programs were understaffed, and services were often limited by long travel distances between CBP facilities and remotely-located technology sites. For example, during January 2020, the OIT's field support operation was authorized 357 southwest border staff positions, but 49 of those positions (approximately 14 percent) were vacant.

The remote location of some positions assigned to certain operating areas has historically made them difficult to fill. Officials from one sector said that only two IT technicians were assigned to maintain CBP's technology systems across an entire sector operating area, which consisted of more than 165,000 square miles in Texas and Oklahoma. Officials said that IT support is regionally assigned, so Border Patrol stations had to schedule and plan for IT service visits in advance, coordinating with every station in the area to ensure all repair needs were included when IT technicians were present in the area. Also, due to the remote locations of field technology placement, technicians often had to spend many hours, sometimes days, traveling the distances between CBP sites and remote technology system locations.

Some Border Technology Systems Did Not Comply with Security Requirements

The DHS *Sensitive Systems Policy*[19] requires that components, including CBP, establish, implement, and enforce configuration management controls on information systems and networks to reduce vulnerabilities. Information systems must be securely configured in accordance with acceptable industry standards, such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs),[20] Center for Internet Security benchmarks, or other recognized industry standards for operating systems and applications. According to the DHS Office of the Chief Information Officer, DHS is currently establishing Department-specific guidelines for information systems controls. However, these guidelines had not yet been implemented at the time of this audit. Until DHS guidelines are published, components must ensure information systems are configured using industry standards (primarily DISA STIGs categories) and applicable DHS configuration guidance, as listed in DHS' *Sensitive Systems Policy,* as the configuration management standard.

[19] *DHS Sensitive Systems Policy Directive 4300A*, July 27, 2017.
[20] Developed by DISA, STIGs are the configuration standards for devices and systems. STIGs contain technical guidance to lock down information systems and software that might be vulnerable to malicious computer attack.

We determined, as part of our review, that CBP implemented a patch management program[21] that deployed software patches to reduce vulnerabilities on tested assets. However, technical assessments conducted by OIG's Information Assurance and Testing (IAT) Branch of 137 assets within the RVSS, ICAD, and e3 authorization boundaries identified 237 instances of 47 unique critical and high severity patch-related vulnerabilities. The IAT Branch also used the DISA STIGs to perform configuration management testing on the three selected systems, revealing that CBP had not fully implemented DHS-approved configuration settings.[22] Compliance with the DISA STIGs guidelines ranged from 38 percent for the e3 system to 99 percent for RVSS system assets. Table 4 lists DISA STIGs category levels and associated levels of severity.

Table 4. DISA STIGs Category Guidelines

Category	DISA STIGs Severity Guideline
I	Any vulnerability, the exploitation of which will directly and immediately result in loss of confidentiality, availability, or integrity.
II	Any vulnerability, the exploitation of which has a potential to result in loss of confidentiality, availability, or integrity.
III	Any vulnerability, the existence of which degrades measures to protect against loss of confidentiality, availability, or integrity.

Source: DISA STIGs Guidelines

Table 5 provides the results of the IAT Branch's assessment testing.

[21] Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware.
[22] DISA STIGs settings are categorized by severity, based on the impact to information or assets, if subverted or improperly configured.

Table 5. DISA STIGs - Failed Controls on CBP Technology Assets

Type of Asset	Number of Failed Controls, by Category		
Workstations	**Category I**	**Category II**	**Category III**
ICAD	9	132	10
RVSS	0	19	2
Servers	**Category I**	**Category II**	**Category III**
e3	7	126	11
ICAD	1	60	5
RVSS	0	18	1

Source: DHS OIG Information and Assurance Testing Branch

The existence of these vulnerabilities indicated CBP had not fully implemented appropriate configuration management guidelines. According to a contracted technology specialist who manages IT security, CBP had not applied patches or ensured compliance with configuration management settings when doing so hindered a system's functionality or performance during normal operations. For example, one of the missing controls identified during our testing required that a specific encryption algorithm be implemented to secure network communications. However, implementing this control would cause video management capabilities to stop functioning, so CBP did not implement the control.

CBP did not comply with existing DHS guidance or acceptable industry standards to ensure proper configuration management controls for its operating systems and applications. Instead, CBP implemented the specific controls that were outlined in the FY 2020 DHS Information Security Performance Plan. This was not adequate. The DHS Office of the Chief Information Officer stated the Information Security Performance Plan is not an official policy document [on par with the *Sensitive Systems Policy Directive 4300A*.] The performance plan merely contains metrics used to track component progress each FY toward achieving departmental goals.

We conducted further inquiry to determine the root cause of the discrepancy between CBP's configuration management approach and Department policy guidance. We were informed by CBP that they, along with other DHS components, had reached a formal agreement with the DHS Council of Chief Information Security Officers to implement a "phased approach" for implementing all DISA STIGs categories as the configuration management standard. According to the CBP Chief Information Security Officer, this change was verbally agreed upon, but not documented. Moreover, CBP did not establish a timeline for completing implementation of the DISA STIG categories.

CBP Needs a Reliable Process to Assess Technology Effectiveness

CBP was not well-equipped to respond to these deficiencies, as it did not have a standard process to assess technology effectiveness in supporting mission operations. Executive Order 13767 directed that DHS use appropriate technology to support the physical wall along the southern border, to most effectively achieve complete operational control. To assess whether effective technology has been selected and deployed to support the border wall, CBP must establish a reliable process to accurately measure technology's performance.

However, CBP has not established a formal process and does not have reliable data to assess technology performance. CBP has been aware of this challenge since at least 2017, when GAO reported that Border Patrol was not well positioned to fully assess its progress in implementing the 2014 *Southwest Border Technology Plan*, and to determine when mission benefits related to technology had been fully realized.[23]

According to program management officials, Border Patrol has attempted to use its existing TSM system to capture technology performance data to assess how effectively technology supports mission operations. Deployed in January 2017, TSM provides near real-time representation of agent activities in the field, including technology use, by tracking technology sensor alerts from the first detection of activity to final resolution. During operations, agents and supervisors enter operational activity data into TSM, including technology asset assists,[24] which attribute the assistance of specific technology system to operational activities, such as apprehensions. According to Border Patrol, through this tracking process, TSM assists Border Patrol in determining which technologies best support positive law enforcement outcomes.

However, numerous Border Patrol supervisors said that TSM cannot be used to effectively assess technology effectiveness due to its unreliable data. Border Patrol's TSM *Internal Operating Procedures* require system users to manually enter accurate and complete data and include all relevant operational and situational awareness information, such as tracking data collected from Border Patrol sensors, during the course of operations. According to field supervisors, however, the quality of TSM data has often correlated to individual agent

[23] *Border Patrol Is Deploying Surveillance Technologies but Needs to Improve Data Quality and Assess Effectiveness*, GAO-18-119, Nov. 2017.
[24] An asset assist occurs when a technology asset, such as a surveillance tower, or a non-technological asset, such as a canine team, contributes to apprehensions or seizures.

interpretations, which supervisors said varied significantly, and frequently resulted in inaccurate TSM records. Officials lacked confidence in TSM's capability to accurately measure technology's contributions to operations. On a daily basis, watch section supervisors and other agents had to manually verify and correct TSM data to ensure integrity. A sector-level TSM supervisor said that data quality management required two full-time staff to perform daily data validations. The supervisor said that to pull just a simple report from TSM, he first had to verify and manually correct event data, such as the apprehension of persons illegally crossing the border.

Technology Shortfalls Impede Complete Situational Awareness of the Southwest Border

CBP may be unable to meet the requirement to deploy appropriate technology to support the border wall for achieving complete operational control of the border.[25] Lacking adequate situational awareness, Border Patrol frequently diverted its limited number of agents from their primary mission duties to patrol areas where planned technology assets had not been deployed or were not available for use. For example, agents from the Rio Grande City Border Patrol Station in Texas spent up to 30 minutes traveling to investigate sensor alerts because no RVSS camera was in place, as planned, to provide video surveillance of a certain area. Similarly, agents from the Brown Field Border Patrol Station in California routinely traveled 45 minutes or more to investigate sensor alerts in vulnerable border areas where no video surveillance capability existed. According to station officials, once agents arrived on site, they sometimes discovered that things like animals or wind gusts had triggered the sensor alerts.

Diverting personnel to areas where technology had not been deployed, along with Border Patrol's already-limited staffing numbers, resulted in missed opportunities for CBP to halt illegal activities, such as illegal crossings and smuggling, along the southwest border. Until CBP increases its field staffing numbers and hires new agents, or systems are better integrated to reduce staffing needs, southwest border stations will struggle to keep pace with operational requirements, including responding to technology in the manner required by mission needs. When stations were understaffed, they had to make operational trade-offs, such as shutting down vehicle checkpoints. To mitigate its field staffing challenges, CBP relied heavily on temporarily-detailed military personnel for support to, for example, operate MVSS trucks in the field

[25] Executive Order 13767, Border Security and Immigration Enforcement Improvements.

for remote surveillance, or operate IFT and RVSS camera system consoles at Border Patrol command centers.

Additionally, Border Patrol agents will face greater safety risks as they are required to patrol areas surrounding the new border wall and physically investigate potential tunnels in place of adequate technology. Agents spent hours or days entering, mapping, and measuring tunnels, which exposed them to significant dangers such as encounters with smugglers, trip wires, and possible tunnel collapse. Stations also dedicated limited staff resources to physically monitoring infrastructure tunnels, which frequently diverted agents from other critical patrol functions.

Further, CBP cannot plan effectively for future investments, including technology selection and field placement, to best meet border security requirements. In FY 2021, for example, CBP expects to spend $28 million to deploy 30 innovative towers, but the component has no process in place to assess the effectiveness of this and other planned technology systems to support current mission operations. As such, CBP is at risk of investing hundreds of millions of dollars in less effective solutions, or deploying technology assets to less optimal field locations.

Conclusion

To achieve complete operational control of the southwest border, CBP requires effective technologies complementing the physical wall as deterrents to people, terrorists, terrorist weapons, and contraband entering the country between lawful ports of entry. However, much work remains for CBP to meet the Federal requirement for deploying the most effective technologies and tools to support the border wall system and further enhance situational awareness by closing existing gaps in border surveillance coverage. Given an environment of limited funding, CBP must deploy new technology in balance with adequate staffing to ensure full utilization of the advanced surveillance capabilities. Leveraging technology to its full capability will improve patrol agents' information sharing as well as situational awareness in border areas lacking coverage. However, fundamental to achieving these objectives is establishing a formal process with reliable data as a means of evaluating technology to ensure limited financial resources are invested wisely. Until progress is made in these areas, CBP will struggle in carrying out its mission of detecting illegal border activities, while also exposing its agents to undue risk.

Recommendations

Recommendation 1: We recommend the Acting Commissioner of CBP update the 2014 *Southwest Border Technology Plan* to identify and prioritize the appropriate technology and funding required to enhance operational control of the southern border.

Recommendation 2: We recommend the Acting Commissioner of CBP develop and implement a comprehensive process for measuring technology's performance to assess its effectiveness in providing situational awareness to fulfill border security mission requirements.

Recommendation 3: We recommend the Acting Assistant Commissioner of CBP's Office of Information and Technology coordinate directly with the DHS Office of the Chief Information Officer to ensure patch and configuration management controls for all information technology systems comply with documented DHS requirements.

Management Comments and OIG Analysis

CBP provided written comments in response to a draft of this report. We reviewed CBP's comments, as well as technical comments, and made appropriate changes to the report. CBP concurred with all three of our recommendations. We have included a copy of the comments in their entirety in Appendix B. A summary of CBP's responses and our analysis follows.

CBP Response to Recommendation 1: CBP concurred with this recommendation and stated that it had completed its Initial Requirements Document–Domain Awareness, which documents capability gaps, operating environments, capability requirements, and notional solutions for all Border Patrol sectors. Signed November 30, 2020, the Initial Requirements Document–Domain Awareness serves as the FY 2021 requirements and prioritization for technology solutions. Additionally, a prioritization initiative was completed to identify which capability gaps, by sector and station, had the greatest need for mitigation. CBP believes this holistic approach will ensure each technology solution is deployed in a manner where the staffing, environment, and other technologies best meet operational needs. According to CBP, the effort to reassess all capability solutions and the associated costs will be an annual requirement for Border Patrol. CBP requested this recommendation be considered resolved and closed, as implemented.

OIG Analysis: We acknowledge Border Patrol's efforts to address and prioritize its border technology planning efforts by implementing the Initial Requirements Document–Domain Awareness. We consider this progress towards meeting the intent of this recommendation, and we look forward to reviewing supporting documentation for these initiatives. We consider this recommendation resolved, but it will remain open until CBP provides documentation showing that all planned corrective actions are completed.

CBP Response to Recommendation 2: CBP concurred and stated that, on October 1, 2020, Border Patrol integrated the Operational Control Framework with the Initial Requirements Document–Domain Awareness. Operational control data was analyzed from pilot stations and briefed to Border Patrol, CBP, and DHS leadership. All southwest border sectors' operational control results were also reported and verified. As part of this effort, the Master Concept of Operations was integrated with the Operational Control Framework, and southwest border operational control metrics were used within the Concept of Operations. According to CBP, the FY 2021 Concept of Operations has been approved to determine the viability of setting southwest border operational control targets.

In addition, Border Patrol will implement the Operational Control Framework across all southwest border sectors, allowing management of situational awareness performance, and supporting initial evaluation and assessment of assets for situational awareness. By July 30, 2021, Border Patrol will utilize existing simulation capability to estimate total flow for use in calculating situational awareness scores for the FY 2020 southwest border operational control. Once complete, Border Patrol will analyze situational awareness scores to better inform asset procurement and/or deployment decisions, develop simulation capability to estimate the impact assets will have on situational awareness, and better inform procurement and/or deployment decisions. CBP expects to complete these efforts by September 30, 2021.

OIG Analysis: We acknowledge CBP's efforts to integrate the Operational Control Framework with the Initial Requirements Document–Domain Awareness, and its plans to implement the Operational Control Framework across all southwest border sectors. We consider these actions positive steps toward addressing this recommendation. We look forward to receiving status updates and documentary evidence as these plans are implemented during 2021. We consider this recommendation resolved, but it will remain open until CBP provides documentation showing that all planned corrective actions are completed.

CBP Response to Recommendation 3: CBP concurred, stating the Office of Information and Technology Cybersecurity Directorate will continue to work with the DHS Chief Information Officer to develop and implement required Security Technical Implementation Guide configurations within CBP, in accordance with DHS policy. Established policy configurations will be implemented within various management systems, such as Active Directory and Puppet, as well as being "baked" into the Windows/Linux Operating System baseline images. CBP expects to complete these efforts by September 30, 2021.

OIG Analysis: We recognize CBP's plan to continue working with the DHS Chief Information Officer to develop and implement required Security Technical Implementation Guide configurations within CBP, in accordance with DHS policy. We look forward to receiving updates and documentary evidence, as these configurations are developed and implemented during 2021. We consider this recommendation resolved, but it will remain open until CBP provides documentation showing that all planned corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107-296) by amendment to the *Inspector General Act of 1978*. We conducted this audit to assess the effectiveness of CBP's current tools and technologies to support Border Patrol's mission operations for preventing the illegal entry of noncitizens who may pose threats to national security.

During this audit, we focused on how effectively CBP has planned and deployed technology systems, IT tools, and IT infrastructure improvements to carry out Executive Order 13767 and fulfill its mission of securing the United States' southwest border by preventing illegal crossings and other criminal activities. We evaluated key technologies and IT systems, tools, and infrastructure, including border enforcement systems, networks and IT infrastructure, tactical and other communications systems, air and ground based surveillance systems, and subterranean surveillance technology.

Our audit scope focused primarily on Border Patrol's mission of securing America's southwest land border between legal ports of entry. We assessed major IT weaknesses that pose significant risks or limitations to current border security mission operations. To assess the cause of identified IT weaknesses, we evaluated the adequacy of CBP's current management structure, guidance, policies, and system controls. We also assessed technology modernization initiatives intended to strengthen border security operations. We did not include technology related to CBP's mission of supporting legitimate trade and travel as part of this audit.

We researched and used Federal, departmental, and component criteria related to CBP's border security mission, responsibilities, and IT effectiveness. We obtained and analyzed reports, testimony, and other documents pertaining to CBP's use of technology to support border security mission operations. Additionally, we reviewed GAO and DHS OIG reports to identify relevant findings and recommendations, and associated CBP follow-up actions.

We collected and analyzed more than 400 documents, and interviewed more than 200 personnel at headquarters and selected field locations, including program office personnel, operational agents, and support personnel such as IT staff, system users, and other stakeholders.

We interviewed CBP headquarters officials and technology personnel within key program offices from Border Patrol, Air and Marine Operations, the Office of Information and Technology, and the Office of Facilities and Asset Management.

We visited various sites within the operating areas of Border Patrol sectors located in Tucson, Arizona; Rio Grande Valley, Texas; and San Diego, California. We also visited the Air and Marine Operations Center at Riverside, California, and conducted teleconferences with senior officials from the Big Bend, Del Rio, El Paso, and Laredo Sectors. During these visits, we interviewed supervisory personnel, field operators, IT specialists, and support personnel. We also observed detainee processing procedures using IT systems, witnessed demonstrations of new technology, and toured areas of responsibility in the field to better evaluate deployed technology assets.

Lastly, we used the work of specialists from our DHS OIG IAT Branch in performing vulnerability assessment testing on selected CBP technology systems to determine whether patch and configuration management programs were in place and operating effectively. The IAT Branch performed vulnerability testing on IT infrastructure assets for three selected CBP systems — RVSS, e3, and ICAD.[26] The IAT Branch analyzed vulnerability scan data to assess whether patch management and configuration management programs were in place and operating effectively, and determine the effectiveness of security controls to protect sensitive system data. The IAT Branch performed vulnerability patch management scans on CBP's e3 database and servers, ICAD workstations and servers, and RVSS workstations and server assets. The results of IAT's work are incorporated as appropriate in our findings.

We conducted this performance audit between October 2019 and February 2020 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.

[26] ICAD is Border Patrol's primary system for tracking agent dispatches and monitoring unattended ground sensors.

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

January 14, 2021

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

1/14/2021

FROM: Henry A. Moak, Jr.
Senior Component Accountable Official
U.S. Customs and Border Protection

Signed by: HENRY A MOAK JR

SUBJECT: Management Response to Draft Report: "CBP Has Improved Southwest Border Technology, but Significant Challenges Remain" (Project No.19-045-AUD-CBP)

Thank you for the opportunity to comment on this draft report. The 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 pleased with the OIG's recognition that technology in the border environment is an invaluable force multiplier for increasing situational awareness. CBP relies on these tools and technologies to support U.S. Border Patrol's (USBP) mission operations in the challenging southwest border environment.

However, CBP is concerned that the OIG's draft report relies on outdated data from fiscal year (FY) 2019 and early FY 2020, and does not consider the significant progress CBP has made to further improve southwest border technologies and enhance its surveillance capabilities and efficiencies along the southwest border. As a result, the report does not provide an accurate picture of CBP's use of southwest border technology today.

For example, USBP's further development of the Operational Control (OPCON) framework continues to provide insight into assessing technological assets. The OPCON framework features specific performance measures for each OPCON element, including situational awareness, and is progressing in using modeling and simulation tools to better understand the operational environment. As development of the OPCON framework continues, USBP grows more effective in understanding the impact various factors, including technology assets, have on operational performance.

In addition to the OPCON framework, USBP is utilizing the newly completed Initial Requirements Domain Awareness Document (IRD-DA), which includes a prioritization strategy finalized on November 30, 2020, and the Surveillance Capabilities Plan. These documents formalize the process to assist management in determining the type and location of technological assets, which will have the most significant operational impact.

The draft report contained three recommendations with which CBP concurs. Attached find our detailed response to each recommendation. CBP previously submitted technical comments addressing several accuracy, contextual, sensitive and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in 19-045-AUD-CBP

OIG recommended that Acting Commissioner of CBP:

Recommendation 1: Update the 2014 *Southwest Border Technology Plan* to identify and prioritize the appropriate technology and funding required to enhance operational control of the southern border.

Response: Concur. In a cross-directorate initiative led by USBP Operational Requirements Management Division, USBP completed the first IRD-DA, plan, which documents the capability gaps, operating environments, capability requirements, and notional solutions for USBP Sectors Nationwide. The IRD-DA was signed November 30, 2020, and serves as the FY 2021 requirements and prioritization for technology solutions.

Along with this document, a prioritization initiative was completed to identify which capability gaps by sector and station had the greatest need for mitigation.

This holistic approach will ensure each technology solution is deployed in a manner where the staffing, environment, and other technologies best meet the operational needs. The effort to reassess all capability solutions and the associated costs will be an annual requirement for USBP.

On January 8, 2021, CBP provided copies of relevant supporting documentation to the OIG. CBP requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2: Develop and implement a comprehensive process for measuring technology's performance to assess its effectiveness in providing situational awareness to fulfill border security mission requirements.

Response: Concur. On October 1, 2020, USBP integrated the Southwestern Border OPCON framework with the IRD-DA. OPCON data was analyzed from pilot stations and briefed to USBP leadership, as well as senior CBP, and Department of Homeland Security (DHS) leadership. All Southwestern Border sectors' line stations OPCON results were also reported and verified. As part of this effort, the Master Concept of Operations (CONOP) was integrated to OPCON, and Southwestern Border OPCON metrics were used within CONOPs. The FY2021 CONOPs have been approved to determine the viability of setting Southwestern Border OPCON targets.

In addition, USBP will implement the OPCON Framework across all sectors along the Southwestern Borders, allowing management of Situational Awareness performance and supporting initial evaluation and assessment of assets for situational awareness. By July 30, 2021, USBP will utilize existing simulation capability to estimate total flow for use in calculating situational awareness scores for the FY 2020 Southwestern Border OPCON. Once complete, USBP will analyze situational awareness scores to better inform asset procurement and/or deployment decisions. Develop simulation capability to estimate the impact assets will have on situational awareness and better inform procurement and/or deployment decisions. Estimated Completion Date: (ECD): September 30, 2021.

OIG recommended that the Acting Assistant Commissioner of CBP's [Office of Information and Technology] OIT:

Recommendation 3: Coordinate directly with the DHS Office of the Chief Information Officer [CIO] to ensure patch and configuration management controls for all information technology systems comply with documented DHS requirements.

Response: Concur. OIT Cybersecurity Directorate will continue to work with DHS CIO in order to develop and implement required Security Technical Implementation Guide configurations within CBP in accordance with DHS policy. Established policy configurations will be implemented within various management systems such as Active Directory, and Puppet as well as being "baked" into the Windows/Linux Operating System baseline images. ECD: September 30, 2021.

Appendix C
Office of Audits Major Contributors to This Report

Craig Adelman, Division Director
Christopher Browning, Audit Manager
Theresa Whitmore, Auditor in Charge
Swati Nijhawan, Senior Program Analyst
W. Mitchell Chaine, Senior Auditor
Thomas Rohrback, Chief, Information Assurance and Testing Branch
Rashedul Romel, IT Specialist
Lindsey Koch, Communications Analyst
Lori Smith, Independent Reference Reviewer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Legislative Affairs
Acting Commissioner, U.S. Customs and Border Protection
Acting Assistant Commissioner, CBP Office of Information and Technology
U.S. 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