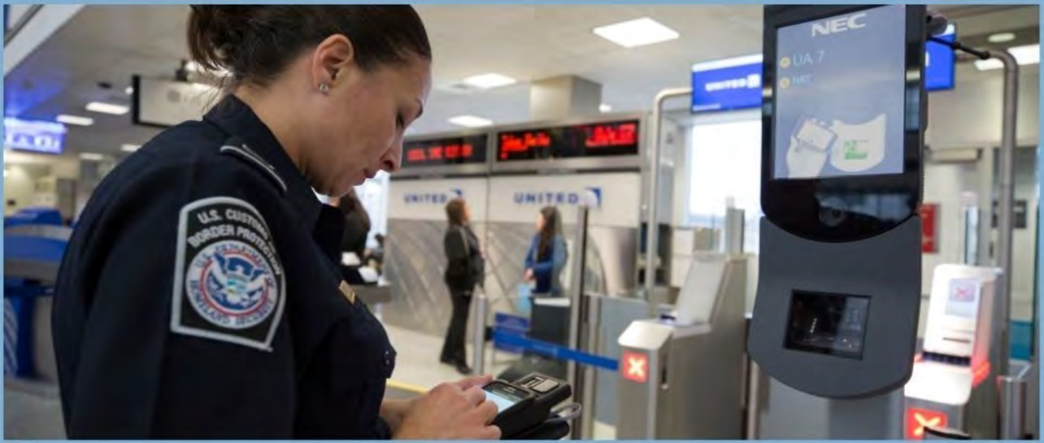
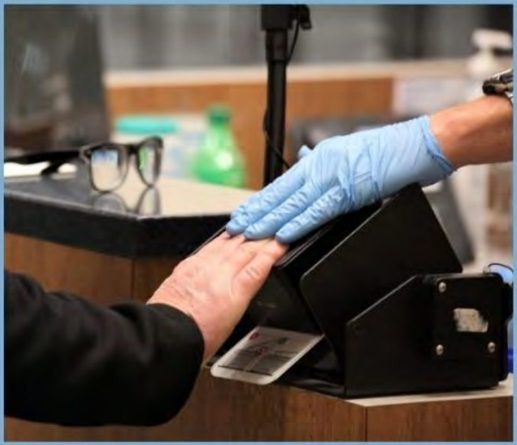




OIT FISCAL YEAR 2020 YEAR IN REVIEW

U.S. Customs and
Border Protection

U.S. CUSTOMS AND BORDER PROTECTION ENTERPRISE SERVICES OFFICE OF INFORMATION AND TECHNOLOGY

TABLE OF CONTENTS

MESSAGE FROM OFFICE OF INFORMATION AND TECHNOLOGY ACTING ASSISTANT COMMISSIONER

I am pleased to present the OIT "Year in Review Report for Fiscal Year 2020 (FY20)." As the largest information technology (IT) organization in the Department of Homeland Security (DHS) with an IT budget of $1.8 billion encompassing 72 investments, 340 projects/systems, and many key high value assets CBP's Office of Information and Technology (OIT) plays a vital role in protecting and supporting our national security and prosperity.

I want to thank former Assistant Commissioner, Phil Landfried, who retired from CBP this past June after 28 years of exceptional service to CBP, and current OIT Acting Deputy Assistant Commissioner Valerie Isbell, who is retiring in December after 37 years of outstanding support to the U.S. Government (17 years at CBP). We wish them both all the best.

The intent of this "Year in Review Report" is to showcase the OIT accomplishments and major milestones reached during FY20 aligned to five strategic focus areas and to provide preliminary insights into the journey ahead. A small subset of highlights are as follows:

Mission Operations: Exceeded IT goals by migrating 91 mission support applications to the cloud; improving IT infrastructure capacity, redundancy; and providing world-class cybersecurity protection to mission programs with top Federal Information Security Management Act (FISMA) scores in DHS

CBP Strategy: Created the overall CBP dashboard for the five Enduring Mission priorities and led the IT Infrastructure Strategic Initiative (1 of 12) exceeding all performance metrics

CBP Statutory Compliance: Improved IT Management by creating a Technology Reference Model, a Technology Innovation partnership with INVNT Program (Industry-to-frontline mission adoption of 11 cutting-edge technology solutions); and inserted 40+ new technologies to meet mission needs. Achieved best-ever scores in FITARA (HR, Budget, Acquisitions, Portfolio), records management visualized through data analytics.

Business Operations: Implemented a rapid COVID-19 response for the CBP workforce of more than 62,400 personnel,COVID-19 tracking/reporting tools, capacity increases, and web conferencing tools to facilitate seamless collaboration for CBP's 24x7x365 global mission.

Trusted Partnerships: Improved Trusted Partnerships and collaboration with stakeholders on five fronts: our collaboration within CBP; across DHS and components; across U.S. Government; our Industry/ Trade partners; and in the CIO Technology Forum with our Five Eye countries: Australia, Canada, New Zealand, the United Kingdom, and the United States to further cooperation on the border and immigration of the future.

I am especially proud of the incredible resiliency and professionalism of the OIT workforce in supporting the mission despite a year of unprecedented challenges. I am committed to ensuring OIT continues to deliver secure and reliable IT capabilities to you, our trusted partners.

For more information or if you have any questions for OIT, please visit our website or email the Communications Team mailbox at OITCommTeam@cbp.dhs.gov.

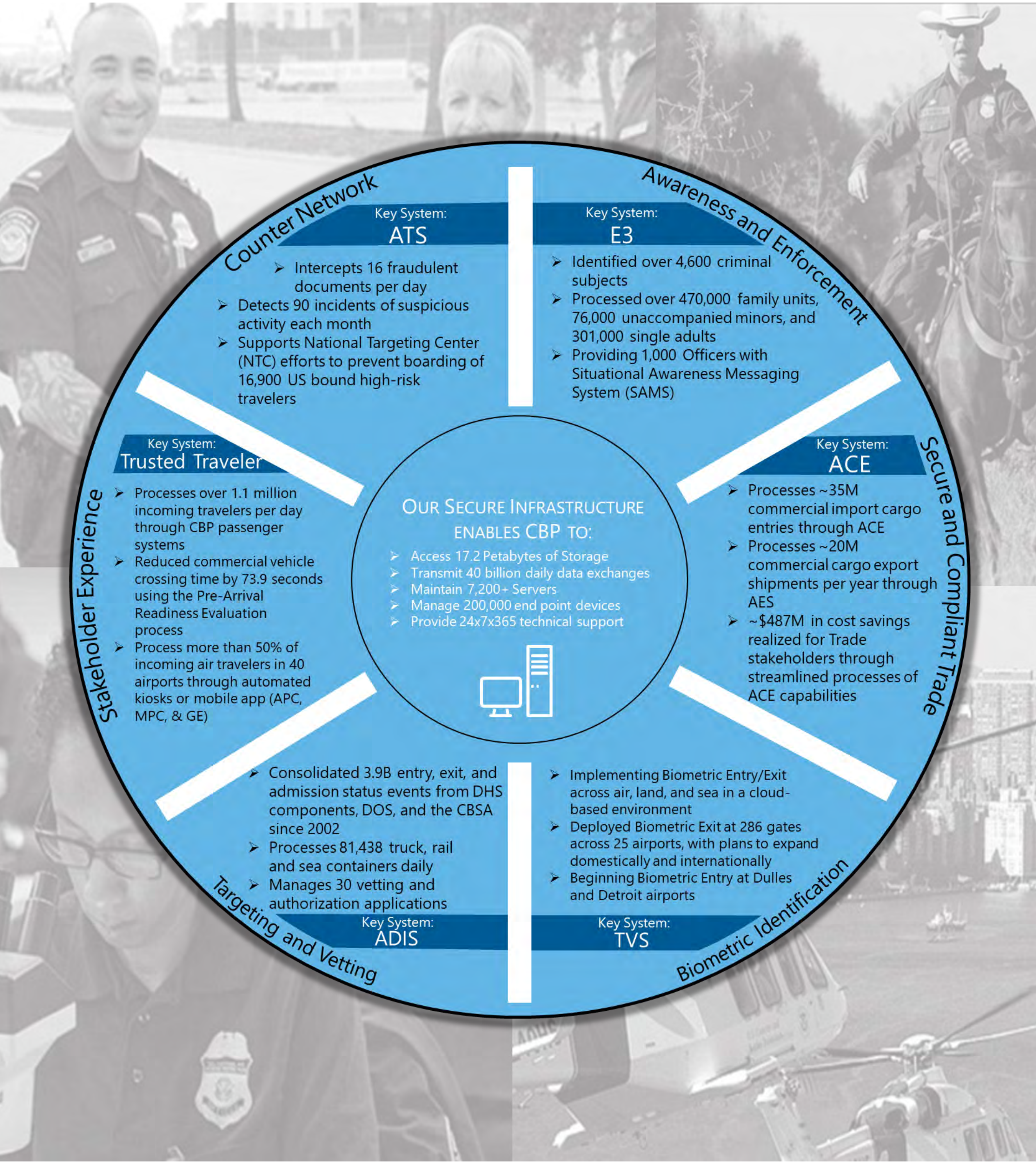
Sincerely,

Sanjeev (Sonny) Bhagowalia

Acting Assistant Commissioner, Office of Information Technology and CIO, CBP

ENTERPRISE OVERVIEW

ENTERPRISE OVERVIEW



Counter Network

Key System: **ATS**

- Intercepts 16 fraudulent documents per day
- Detects 90 incidents of suspicious activity each month
- Supports National Targeting Center (NTC) efforts to prevent boarding of 16,900 US bound high-risk travelers

Awareness and Enforcement

Key System: **E3**

- Identified over 4,600 criminal subjects
- Processed over 470,000 family units, 76,000 unaccompanied minors, and 301,000 single adults
- Providing 1,000 Officers with Situational Awareness Messaging System (SAMS)

Stakeholder Experience

Key System: **Trusted Traveler**

- Processes over 1.1 million incoming travelers per day through CBP passenger systems
- Reduced commercial vehicle crossing time by 73.9 seconds using the Pre-Arrival Readiness Evaluation process
- Process more than 50% of incoming air travelers in 40 airports through automated kiosks or mobile app (APC, MPC, & GE)

Our Secure Infrastructure enables CBP to:

- Access 17.2 Petabytes of Storage
- Transmit 40 billion daily data exchanges
- Maintain 7,200+ Servers
- Manage 200,000 end point devices
- Provide 24x7x365 technical support

Secure and Compliant Trade

Key System: **ACE**

- Processes ~35M commercial import cargo entries through ACE
- Processes ~20M commercial cargo export shipments per year through AES
- ~$487M in cost savings realized for Trade stakeholders through streamlined processes of ACE capabilities

Targeting and Vetting

Key System: **ADIS**

- Consolidated 3.9B entry, exit, and admission status events from DHS components, DOS, and the CBSA since 2002
- Processes 81,438 truck, rail and sea containers daily
- Manages 30 vetting and authorization applications

Biometric Identification

Key System: **TVS**

- Implementing Biometric Entry/Exit across air, land, and sea in a cloud-based environment
- Deployed Biometric Exit at 286 gates across 25 airports, with plans to expand domestically and internationally
- Beginning Biometric Entry at Dulles and Detroit airports

ENTERPRISE OVERVIEW:
OIT FY20 ACCOMPLISHMENTS AND IMPACT

Successfully helped Industry-to-Frontline adoption of 11 cutting-edge tech solutions through INVNT, e.g. the TAK, which provides officers with real-time situational awareness

Initiated the Trusted Partnership Engagement to build relationships and ultimately support mission success

Migrated over 75,000 mailboxes and 10,000 distribution lists to Office 365 for increased mobility

Working to establish an IT Governance Council to enhance governance of CBP's IT/Information Risk Management (IRM)

INITIATIVES AND INNOVATION

AS OIT RAMPS UP ITS EFFORTS, FY20 HAS SHOWN SOME OF THE MANY BENEFITS OF OIT'S ONGOING INVESTMENTS IN MODERNIZATION

NTC's use of Robotic Process Automation (RPA) saved airlines an estimated $371M in the first ten days of implementation

Secured $15M in TMF funding for ACE Collections Modernization

Migrated 91 applications to the cloud

Sponsored and facilitated Cost Wise Readiness baselining for all 16 ES programs to completion

ENTERPRISE OVERVIEW:
OIT FY20 ACCOMPLISHMENTS AND IMPACT

Upgraded ACE DB2 database to High Availability Disaster Recovery (HADR) databases and deployed East/West ICPs and 4G cellular back-up at ~**200 sites**

Deployed **83** applications in the cloud, of which over 85% are cloud native or low complexity

Deployed **156** TDYs and completed 30+ site visits to execute priority requests and ensure continued equipment resiliency and reliability

~2,000 daily calls to the Technology Service Desk

24/7 operations and maintenance

Increased network speed and resiliency for **400+ circuits** at USBP, OFO, and AMO sites by upgrading circuits, refreshing switches, and installing 4G backups

Finalized an IP Address roll out for more than **2,700** devices that enhanced their security

Enable **40 billion** daily data exchanges with other government agencies, passenger carriers, cargo brokers, and trade users

Implemented a modern security architecture to ensure resilient and high-performing connectivity

OIT executed FY20 budget of **~$1.5B** (*This includes investment & non-investment funding). AC/OIT & CIO oversees and manages CBP's IT and mixed IT portfolio of **$1.77B**

METRICS AT A GLANCE

OIT continually hits the mark and improves year after year through discipline and strong guidance from leadership.

OIT's latest **FISMA scorecard** was overwhelmingly positive with 13/13 metrics scoring an average of: **97%**

Partnering with HRM and The Hiring Center enabled OIT to achieve its **best ever hiring percentage** at: **92%**

OIT'S COVID-19 SWIFT RESPONSE

In just **3 days**, OIT developed the COVID incident tracker with real-time incident management, enhanced executive reporting and dashboards, and rapid scalability for use by ICE and DHS.

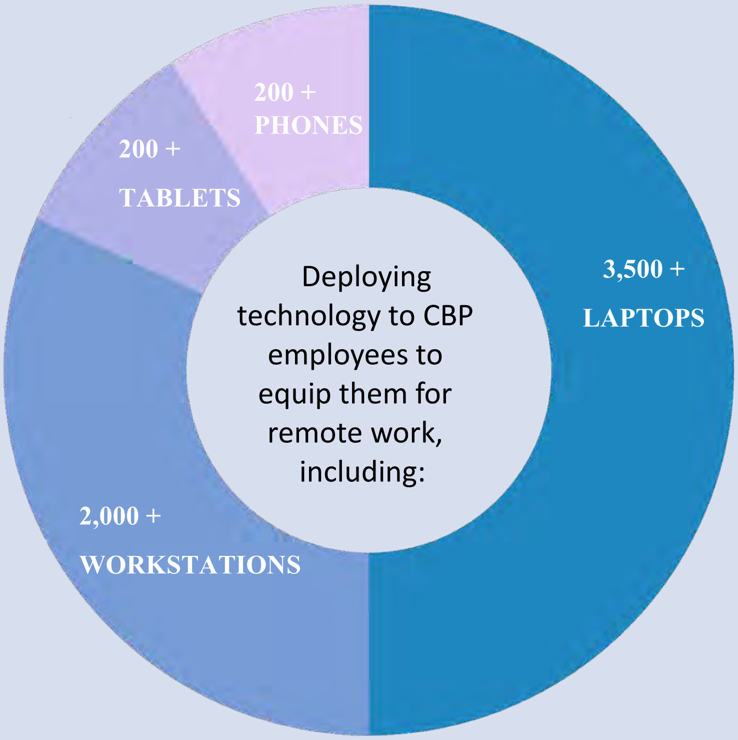
Enabling a Remote Working Environment

To support the surge of personnel that would be shifting to telework, OIT acted swiftly by:

Installing **300 new phone lines** and over **2,000 new WebEx host accounts** to support the increased request for conference lines and WebEx usage.

Implementing **GlobalProtect** as an alternative VPN solution to ensure CBP users can securely connect to the network, providing an additional telework capacity for up to **48,000 users**

Facilitating weekly trainings that reached over **7,000 people** to ensure employees took advantage of available **collaboration tools**


Deploying technology to CBP employees to equip them for remote work, including:

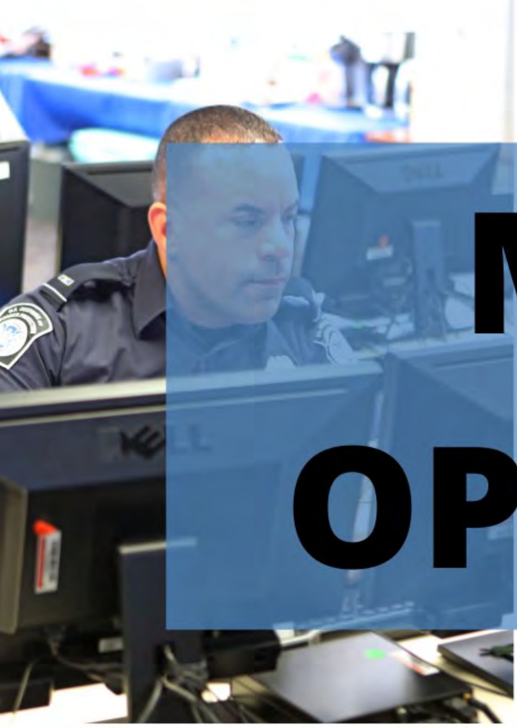
USBP- Supported the set up of open-air **temporary processing areas** with network-capable workstations to help reduce spread of COVID-19

OFO- Developed a **contactless inspection** solution for the Massena Port of Entry in NY, allowing operators to process travelers without machine readable travel documents

OT- Deployed the expedited **Automated Commercial Environment (ACE) release** to implement duty deferral executive order

AMO- Deployed two **Qlik dashboards** to monitor surge operations for virus-related border activity and gain insight into COVID-19 impact comparison statistics

MISSION OPERATIONS

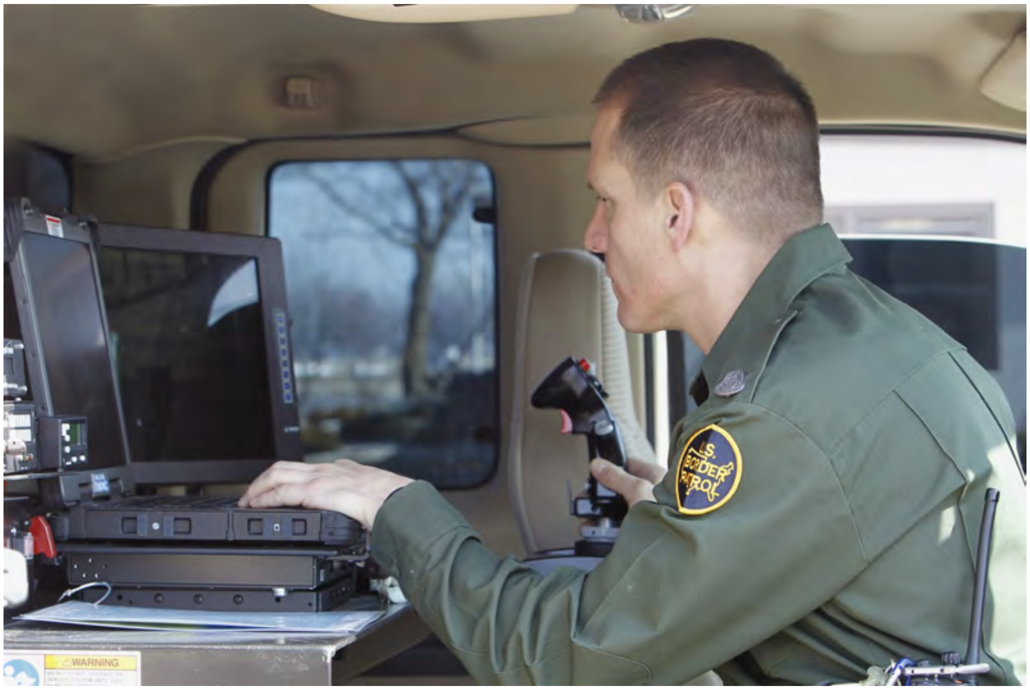


ENFORCEMENT AND SOUTHWEST BORDER SUPPORT

The Enterprise Networks and Technology Support Directorate (ENTSD) is responsible for the architecture, design, implementation, and management of CBP network infrastructures. Field Support Directorate (FSD), the operations and maintenance organization, is responsible for information technology, tactical radio communications, and surveillance systems. Together, ENTSD and FSD modernized and provided invaluable technology support capabilities along the U.S. southern border, despite the fact that FY20 has been a year like no other for safeguarding the southern border with the need for social distancing, mobility for alternate work locations, and expanded use of technology for crisis response.

To minimize disruption to the Land Mobile Radio (LMR network, the ENTSD team installed and implemented Dynamic System Resiliency (DSR), a fully redundant backup infrastructure for the LMR network, to improve system survivability. At the Big Bend Sector and Lordsburg Border Patrol stations in Texas and New Mexico, respectively, the team activated and integrated GPS into the Enterprise Geospatial Information Services application (eGIS) in 200 mobile and 270 portables radios on the LMR network to enhance situational awareness and officer safety. ENTSD replaced 197 end-of-life routers and 15 switches on the LMR network and Cellular Over the Horizon Enforcement Network (COTHEN), significantly improving the connectivity, reliability, and security of mission-critical border communications. These investments in critical infrastructure helped ENTSD achieve 98% reliability for both the LMR network and COTHEN, further enabling mission-critical communications in remote operating environments. ENTSD logistical improvements to CBP's infrastructure included the installation of approximately 1,250 new cameras and 350 microphones across 29 U.S. Border Patrol (USBP) and Office of Field Operation (OFO) sites, improving situational awareness and increasing CBP's ability to provide recordings of interactions with the public.

ENFORCEMENT AND SOUTHWEST BORDER SUPPORT



Through collaboration with the Department of Justice and U.S. Immigration and Customs Enforcement (ICE), ENTSD and FSD continued to support the Migrant Protection Protocol (MPP) Immigration Hearing Facilities (IHF) in Laredo and Brownsville, Texas. Both locations are targeted to modernize to permanent facilities in FY21. The teams supported the rapid installation of hardware in response to the influx of individuals on the southwest border and resultant MPP processing. Soft-sided tent holding facilities from San Diego, California to Brownsville, Texas expanded in size and capacity, from being able to hold 500 to holding 3,000 migrants. FSD and ENTSD completed multiple requests to ensure full mission capability at each site through May 2020. Once the soft-side facilities were decommissioned, FSD removed and stored all technology for rapid recommissioning of the site.

The advent of COVID-19 required a different approach to holding and processing migrants. The Office of Facilities and Asset Management (OFAM) deployed clamshell type tents, called CAMs, to numerous locations across the southern border, enabling U.S. Border Patrol (USBP) stations to process and isolate those testing positive for or showing coronavirus symptoms. FSD outfitted each of the CAMs with network connectivity and equipment, providing agents a fully operational alternate site.

FY20 HIGHLIGHTS

In FY20, ENTSD deployed and maintained over 78,000 pieces of surveillance equipment.

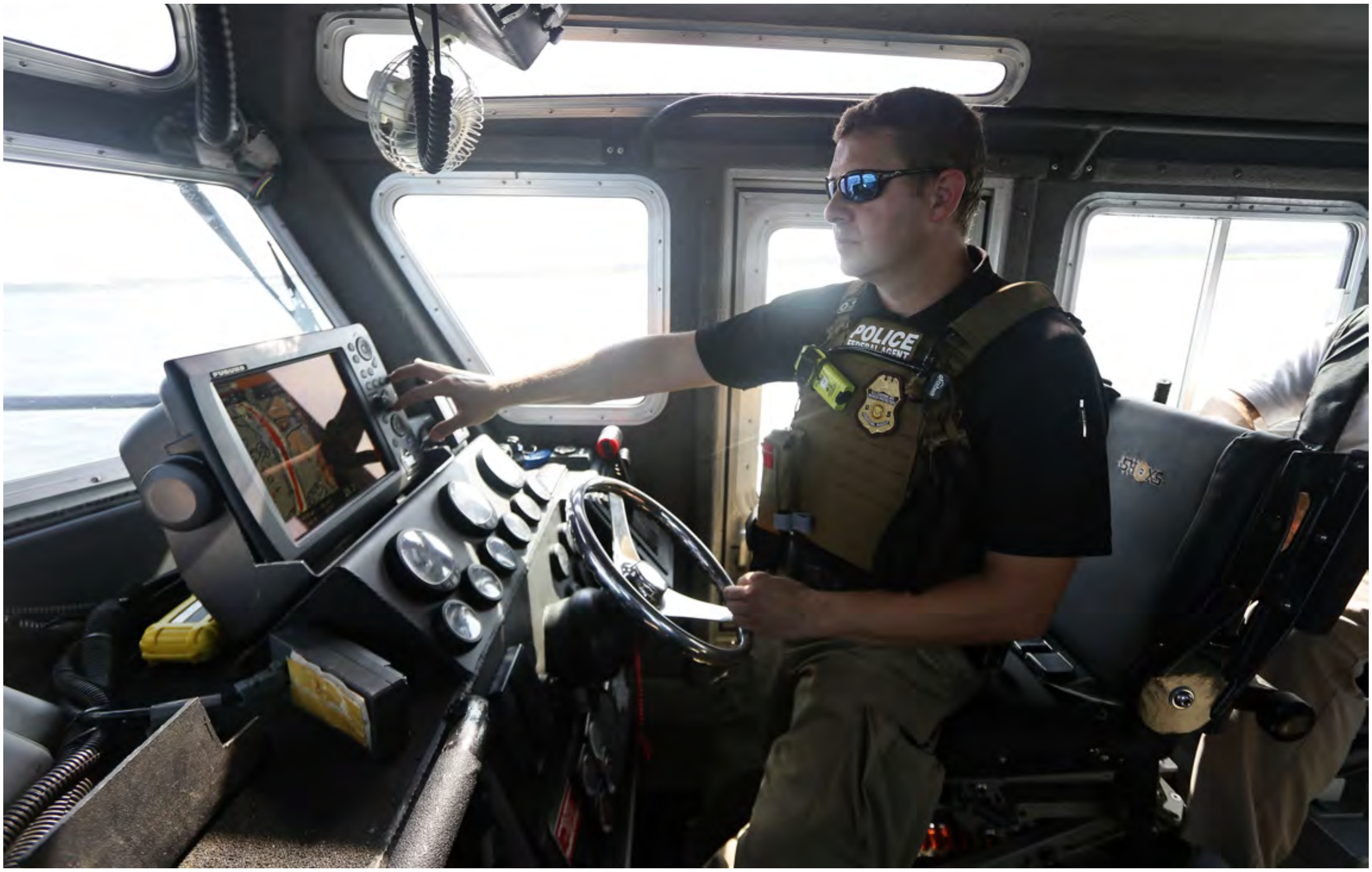
The Technology Service Desk completed over 100,000 service tickets in support of information and enforcement technologies.

Hurricanes Hanna and Laura resulted in numerous outages in the Eastern zone near the Gulf of Mexico. FSD and ENTSD completed site resolution cases within days of each storm passing.

Completed 123 circuit upgrades to Integrated Communication Provider (ICP), dramatically increasing bandwidth, availability, and positive user experience.

Installed new solid state hard drives and RAM to every CBP E3 processing machine along the southern border after identifying computer desktop and hardware shortfalls.

ENTERPRISE ANALYTICS



The Targeting and Analysis Systems Program Directorate (TASPD) supports the CBP targeting enterprise in securing the nation’s borders while facilitating legitimate travel and trade. TASPD is responsible for improving, administering, and maintaining selectivity, targeting systems and related systems that help secure the supply chain and support CBP's layered defense strategy for international cargo and passengers.

The TASPD Advanced Analytics team collaborated with the Office of Field Operations (OFO) and its National Targeting Center (NTC), as well as OFO’s Planning, Program Analysis and Evaluation (PPAE) and Tactical Analytic Units (TAUs), the Office of Trade (OT), ports of entry (POEs) and other stakeholders, to analyze, design, develop, and implement innovative, risk-based decision support tools, including predictive and scenario-based models, visualization applications, and performance reporting. The team provided robust subject matter expertise in threat research, quantitative network analytics, and *ad hoc* query. Ultimately, TASPD Advanced Analytics made significant contributions to intelligence-driven, risk-based targeting efforts and operations in direct support of CBP, as well as interagency and international partners.

The team deployed several brand new risk models to address specific operational needs, which includes the design, development, and deployment of the National Security Inbound (NSI) -Watchlist Service (NSI-WLS) model, all in an extremely compressed schedule of under four weeks.

ENTERPRISE ANALYTICS

The NSI-WLS model limits query results to low volume consignees or shippers when the target volume becomes too high for field operations, adds a critical targeting feature within the Automated Targeting System (ATS), and is leveraged across Advanced Analytics' suite of NSI-models to drive targeted shipments to hotlists at the NTC. In addition, the team deployed an enhanced NSI-Maritime (NSI-M) model, as well as an inaugural Truck Crew Narcotics Risk Model (TCNRM) to complement existing commercial truck targeting. For further enhancement of trade targeting and enforcement, the team deployed a revised Tariff Evasion Model and Importer Risk Dashboard to provide a more holistic analysis of potential revenue recovered. The trade modeling team also developed a new Post Summary Correction (PSC) recovery model to provide OFO with further risk analysis of entry summaries that potentially owe additional revenue to CBP. In addition, the team developed and executed significant enhancements to a portfolio of southwest border narcotics targeting models, and developed two new scenario-based national security models (NSI-WLS and NSIM).

FY20 HIGHLIGHTS

130 ocean cargo intellectual property rights (violation seizures totaling $45,149,152 in MSRP

203 air express cargo drug seizures totaling 220 kg

16 truck cargo drug seizures totaling 16,946 kg

341 passenger rug seizures totaling 3,038 kg

TASPD Advanced Analytics added various enhancements to its data analytics and model deployment capabilities by leveraging modeling tools, such as SAS and DataRobot, along with the development of improved capabilities within its organic hosting platforms, including Passengers (PAX)/Land Model Operations / Land Model Environment (LME) and the Cargo Model Operations Application / Cargo Model Management System (CMMS). The culmination of these changes resulted in improved development and deployment timelines while seamlessly integrating into existing ATS-workflows. To modernize and to capitalize on the newest capabilities, Advanced Analytics completed the migration of its applications to Amazon Corretto, a multiplatform, production-ready distribution of the Open Java Development Kit (Open JDK) that includes performance enhancements and security patches, fixes, and updates.

Encountering and combating the sudden emergence and rapid spreading of COVID-19 in FY20 placed significant and unrelenting demands on CBP resources. CBP is at the forefront of collaborating with essential partners in fighting the pandemic, aiding in the identification of high-risk travelers, uncovering fraudulent or unsafe Personal Protective Equipment (PPE), and identifying potential vaccine-related intellectual property rights (IPR) infringement. TASPD Advanced Analytics undertook many critical initiatives to augment risk-based decision making, workload management, and performance monitoring capabilities in direct support of the agents, officers, and trade and intelligence professionals in the field to address unique challenges from the COVID-19 pandemic, as well as to carry out the important border security mission.

ENTERPRISE ANALYTICS

The Cargo Systems Program Directorate's (CSPD's) Enterprise Analytics team provides the platform from which CBP comprehensively and insightfully executes its mission to foster lawful trade as well as the collection of duties, fees, and taxes. CBP's High Performance Analytic Appliance (HANA) in-memory platform hosts the data necessary for Automated Commercial Environment (ACE) reporting and integrates the data sources necessary to support the Advanced Trade Analytics Platform (ATAP) program. Critically, CSPD shifted HANA from an on-premises infrastructure to the cloud, thereby complying with Chief Information Officer (CIO) directives, but also leveraging the distributed computing and resiliency provided by the cloud. CSPD shifted HANA to the cloud infrastructure and simultaneously increased the number of data sets. CBP's Trade Transformation Office (TTO) has received numerous testimonials that express the users' gratitude for the HANA platform, as it processes queries more quickly, enabling users to execute increasingly complex queries against increasingly large data sets. In short, users can perform their jobs more efficiently, more effectively, and more comprehensively.

In support of the OT mission, CSPD designed the architecture of the ATAP so that the solution will provide OT with a single, organized point of access for all of CBP's internal and external sources of data. The ATAP solution will rely on a cloud infrastructure and invoke the hybrid "Best of Breed" methodology for incorporating additional technologies. CSPD deployed Databricks in order to assess its capability as a data lake and data hosting platform. Databricks invokes the advantages of distributed computing and advanced data engineering which allow for all CBP data to remain in one central repository. Critically, the Databricks technology avoids any vendor lock-in while also leveraging in-memory processing that provides real-time descriptive, diagnostic, predictive, and prescriptive analytics at both a tactical and strategic level. CSPD will compare the technical attributes and capabilities of Databricks and HANA in order to build the most robust and resilient foundation for ATAP.

FY20 HIGHLIGHTS

Established HANA (development, SAT, and production environments) on cloud infrastructure while maintaining on-premises operations.

Implemented Risk Based Bonding (RBB) solution in furtherance of initial ATAP goals.

Implemented Databricks proof-of-concept and populated it with data to support section 321 analytics and to initiate comparison of Databricks and HANA capabilities.

Expanded CBP's use of in-memory data warehouse technology that provides faster processing of large volumes of CBP data

MOBILITY AND APP DEVELOPMENT

OIT is dedicated to providing CBP operators the necessary mission-critical tools to promote mobility. In FY20, OIT continued to modernize network mobility by expanding device management systems and mission critical application support for the field. ENTSD and the Office of the Chief Technology Officer (CTO) played critical roles in the development, deployment, and management of mission critical applications to enhance situational awareness in the field, support sharing of information internal to CBP, and promote the public to use CBP applications.

To continue CBP's mission to modernize network mobility, ENTSD migrated over 8,000 Android devices from Android KNOX to Android Enterprise in only six months. Android Enterprise's mobility platform system increases certificate management, secures mobile devices from insider threats, establishes per-application Virtual Private Networks (VPNs) and enhances security by separating work and personal data. AirWatch continues to provide better security and compliance of mobile devices through Personal Identify Verification (PIV) credentials to access CBP information. AirWatch also allows for greater access to CBP mobile applications, giving users the tools they need on the go.

OIT launched, updated, and developed multiple mobile applications for CBP in FY20, and CBP currently manages over 24,000 active devices, and 400,000 applications installed through AirWatch. Two examples of apps that provide timely access to relevant CBP information as well as situational awareness are Wickr and Android Team Awareness Kit (ATAK). Wickr is an encrypted messaging application for sharing information in a secure environment. Users can create and use secure rooms in Wickr for messaging, video chat, as well as file, video and photo transfers. In partnership with the CBP Innovation Team, the OFO Field Transformation Team (FT2) and the Area Port of San Francisco (SFO) are piloting Wickr as a potential solution to enhance the dissemination of real-time threat information. ATAK, a secure, map-based application similar to Google or Waze, provides CBP agents and partners in the field with technology features that enhance situational awareness, field safety, and the ability to fulfill their job more efficiently during border incursion incidents. ENTSD migrated all ATAK users to the CBP Amazon Web Services (AWS) Cloud East (CACE) environment and off of external agency SUNet.

MOBILITY AND APP DEVELOPMENT

OIT also launched the myCBP mobile application, ATS Mobility Suite, NextGenTrac, Tririga, miSTAT, BeOn, Workforce for ArcGIS, and Tactical Air, Land & Marine Enterprise Communications (TALMEC). These applications provide CBP employees with access to timely internal CBP information disseminated by CBP leadership. Information assisting in tactical awareness, inspections at ports of entry, biometric scanning for exit encounters, and rapid, real-time communications capabilities. In response to the COVID-19 pandemic, OIT supported the Office of Training and Development (OTD) Field Operations Academy at the Federal Law Enforcement Training Center (FLETC) with the deployment of a custom iPad configuration. The custom deployment streamlined trainee onboarding by pre-registering students, simplifying identity access management, and remotely deploying essential learning applications. The iPads allowed for flexibility never before offered during the traditional training program, and enabled students to disperse safely throughout the FLETC grounds and dorms while using WebEx and Microsoft Teams for lectures and testing.

Electronic Flight Bags for Air and Marine Operations enable mobile devices that carry mission critical data related to a pilot's upcoming flight plans, airport information, weather data, reference data and manuals to be read on an iPad. This has streamlined efficiencies, reduced weight, and provided backup capabilities to the pilot's aeronautics used during mission flights.

The CTO directorate serves as CBP's resource for the identification and creation of novel technology products. CTO creates these novel products using agile methodologies and open standards while in continuous communication with product stakeholders and incorporating end user requirements. CTO's products help to increase efficiency, streamline mission processes, promote transparency, and strengthen CBP operations.

FY20 HIGHLIGHTS

The CBP ROAM application allows travelers entering the U.S. through remote areas to conveniently report their arrival by submitting required information to CBP to fulfill U.S. reporting requirements. ROAM consists of the CBP ROAM Mobile app, the ROAM officer-facing app, and the ROAM Monitoring Dashboard. In FY20:

50% of officer focus was redirected to mission operations and enforcement activities

30,000 trips were successfully submitted through CBP ROAM in FY20

1,320 Local Boater Option requests were approved

The CBP Technical Reference Model (TRM) serves as a catalog of all vetted and approved CBP IT assets, and is updated daily as Technology Insertions (TI) are approved. Originally housed on SharePoint, the CTO team migrated the TI process and TRM to the ServiceNow platform, which provides end users easier ways to view vetted technologies and make formal requests for technologies to be included in the CBP TRM. The ServiceNow platform provides a more friendly and transparent user interface for end users and TRM administrators alike. CTO successfully transitioned the TRM from SharePoint into ServiceNow, which involved the migration of over 10,000 records from the SharePoint TRM onto the ServiceNow platform. The TRM team streamlined the technology review process by updating the Technology Advisory Group (TAG) to include stakeholders from all OIT directorates.

MOBILITY AND APP DEVELOPMENT

CTO created the Robotics Process Automation (RPA) Center of Excellence (CoE) to facilitate the development and propagation of RPA applications throughout the enterprise. RPA software "robots" perform routine business processes by mimicking the way that employees interact with applications and following simple rules to make decisions. The robots are best suited for processes with repeatable and predictable interactions with IT applications, such as opening email and attachments, logging into web/enterprise applications, moving files and folders, filling in forms, copying and pasting, extracting data from the web, making calculations, extracting structured data from documents, collecting social media statistics, and following if/when decisions or rules are implemented/made.

The RPA team developed a "Chile Bot" as a proof of concept with the NTC. The Chile Bot scrapes law enforcement data from Chile to stop applicants from entering the country with illegal or fraudulent applications. On the first day of bot execution, over 1,100 applications were found using illegal National ID numbers. Visas issued in response to those applications were canceled immediately. The bot scraped webpages for over a year's worth of data in less than three days and used RPA to augment missing data fields using data from a public genealogy site.

In March, the team assisted NTC personnel in developing a robot in response to the COVID-19 related Schengen travel ban affecting all travelers who are not U.S. citizens or legal permanent residents. NTC and the RPA team established a new method for processing passengers, designed, developed, and tested four separate automations to work in sequence, and trained chief watch commanders and targeting personnel. Prior to the travel ban, NTC activities led to the removal of less than 100 passengers per day in a process that required between 10 and 15 targeting personnel per shift. Twelve days after the travel ban had been initiated, NTC activities led to the removal of over 230,000 potential travelers prior to boarding and the cancellation of over 3,000 flights.

FY20 HIGHLIGHTS

OIT continued to develop and launch Situational Awareness Messaging System (SAMS), CBP Translate, and Reporting Offsite Arrival – Mobile (ROAM). The SAMS app is a centralized communications application that enables field operators to stay connected and maintain situational awareness. SAMS consists of the mobile app and the Dashboard web app, both of which were enhanced in FY20.

The CBP Translate application is a speech transcribing application aimed at mediating communication between travelers and CBP Officers during interviews. As of FY20, the app offers support for over 130 languages which eliminates language barriers and the need to call in translators often not immediately available during the vetting process. The app is currently being piloted in six airports.

UNIFIED IMMIGRATION PORTAL

The Unified Immigration Portal (UIP) connects relevant data from agencies across the immigration lifecycle to enable a more complete understanding of an individual's immigration journey. Following the surge at the U.S. Southwest border in Summer 2019, the Office of Management and Budget (OMB) identified the need to address challenges posed by a lack of information-sharing within the U.S. immigration system. In response, the Department of Homeland Security (DHS) conceived UIP as an interagency solution, and CBP OIT's Border Enforcement and Management Services Division (BEMSD) took the lead in standing up the program.

UIP has been in lock-step with stakeholder partners across CBP, U.S. Citizenship and Immigration Services (USCIS), ICE, and the Department of Health and Human Services (HHS) to identify use cases and requirements, test developed capabilities, and jointly brief executive audiences such as the House and Senate Appropriations Committees (HAC/SAC), National Security Council (NSC), and Executive Office of the President (EOP). To date, UIP has deployed four dashboards and Timeline View as part of the visualization solution, made data sharing services available to users, and connected four agency systems including CBP e3, ICE Enforcement Integrated Database, USCIS Global, and HHS Unaccompanied Alien Children PATH.

Within a year of standing up the program, UIP's advanced analytics and capabilities have had a direct impact on mission users across agencies with a role in the immigration ecosystem. Earlier this year, the team quickly identified the need for CBP and ICE to proactively manage and respond to potential exposures to COVID-19 and other disease outbreaks. Shortly after, UIP deployed Contact Tracing to enable agents and officers to trace origins of COVID-19 exposures to specific facilities, transfers, or subjects-in-custody. These capabilities have been used in the field to respond to urgent requests regarding subjects who have tested positive for COVID-19 after being released from custody, suspected of having COVID-19 while in custody, or having potential exposure to diseases.

UNIFIED IMMIGRATION PORTAL

UIP has also brought mission-value by sharing near real-time Unaccompanied Alien Children (UAC) data between CBP and HHS such as background information, separations, reunifications, placements, and referrals through the UAC Coordination Dashboard and UAC Referral Service. With UIP, the HHS Intakes Team has additional context it did not have before to place UACs in appropriate facilities rapidly, which helps to reduce wait times and Time in Custody (TIC). These capabilities also help CBP and HHS more quickly and accurately respond to findings from pressing government audits and legal cases, such as the Ms. L case.

Since retiring the code name Athena in July, the UIP user base has grown over 60% and now consists of nearly 1,400 individuals. To achieve this, the team held a formal pilot to rollout UIP to initial groups within the ICE San Antonio (SNA) field office and will soon launch within CBP's OFO. Throughout these pilots, the team directly engaged users to understand their workflow and determine where and how UIP can provide the most impact. Outside of the pilots, the team has also conducted 24 user-experience sessions to collect feedback, prioritize future enhancements, and identify new requirements. In these sessions, users expressed how UIP has reduced the level of effort to complete administrative tasks and provided additional insight into their daily processes. For example, an OFO chief program manager reported they are able to cut time spent on reporting by 50% by using the MCAT Dashboard.

Looking ahead, the program is focused on developing and finalizing the UIP back-end architecture solution, as well as expanding across the program's interagency partners. Along with CBP, the DHS Office of Policy, ICE, and the DoJ have requested funding in support of UIP. The program will work with each of these groups to ensure that the UIP solution meets the needs and requirements of each agency with a role in the immigration system.

FY20 HIGHLIGHTS

Deployed the UIP visualization solution to CBP, ICE, USCIS, and HHS, that integrates interagency data and depicts key information through 4 dashboards and the Timeline View

Grew user base by 60% through tailored rollout plans, demos, and trainings for agency user groups to increase user adoption

Deployed Contact Tracing capabilities for CBP and ICE agents and officers to **proactively manage and respond to COVID-19 and other disease outbreaks across facilities**

Provided HHS users access to a DHS platform for the first time, allowing HHS to use near-real time information such as the UAC Coordination Dashboard

Implemented a suite of **reusable services** with developer-focused content to improve collaboration and integration across mission systems

Analyzed 60 Million data entries for predictive models, contact tracing and forecasting in the UIP graph database

Launched development of UIP's back-end architecture solution, to **enable sharing of UIP visualization and analytics services across agencies**

PASSENGER PROCESSING

The Passenger Systems Program Directorate (PSPD) provides the application development of and operational support for CBP passenger and immigration management systems. PSPD delivers and sustains technology solutions that ensure the safety and security of travelers entering and exiting the US, while facilitating and streamlining legitimate travel. PSPD works to provide CBP, DHS, and stakeholder enforcement agencies with the data they need, when they need it, to support and accomplish the important mission of protecting travelers, trade, and the nation.

PSPD continues to leverage advanced data networks to accelerate mission achievement, simultaneously enhancing the traveler experience and improving security at our nation's borders. In FY20, PSPD moved forward with biometrics-based technologies and data analytics that not only ensure consistent, positive identification of all travelers, but help identify bad actors before their arrival at or between the ports of entry. PSPD also moved forward with a number of cloud-based transitions, with applications and systems moving onto a platform that allows a scalable, agile response that can easily adjust to changing mission needs. In the first half of FY20, PSPD moved several applications and systems either to the on-premises cloud, or to the CACE-environment. In October 2019, PSPD began the ten-month long process of moving the Traveler Documentation and Encounter Data (TDED) program, a central repository of travel documents, arrivals and departures, and Form I-94 Arrival/Departure Record, to the CACE environment. In FY20, Simplified Arrival for Pedestrian (SA-PED) was enhanced to enable issuance of I-94s for travelers with or without prepaying, and without or without fingerprints. SA-PED was also enhanced to enable the officers in the Permit Office to print and collect I-94 fees without re-adjudicating the enforcement hits that had already been performed by the primary officer. In November, the Electronic System for Travel Authorization (ESTA) was redesigned and migrated to CACE. ESTA works to enhance aviation security and reduce border traffic by screening travelers and determining their eligibility for the Visa Waiver Program (VWP).

PSPD also implemented several biometrics-based projects that allow for faster traveler processing using a simple fingerprint or eye scan as opposed to a detailed inspection of travel documents. Biometrics scans also make documentation much harder to falsify, and result in fewer data entry errors at POEs. The Global Entry Next Generation initially will focus on facial recognition technology at the POEs to verify the identity of the Global Entry participants. It utilizes photo comparison from CBP holdings that give CBP officers the ability to conduct faster and more efficient passenger processing. The Primary Inspection Division continued the rollout of Simplified Arrival to ports across the country, and as the new Simplified Arrival application incorporates advanced facial recognition technologies into the primary inspection to expedite the entry process, it will eventually replace Traveler Primary Arrival Client (TPAC) and TPAC-Face as the primary application in Air and Sea Entry processing.

PASSENGER PROCESSING

The COVID-19 pandemic was the catalyst for PSPD to modify several applications used to process data at POEs around the country. In early March 2020, PSPD updated the Consolidated Secondary Inspection System (CSIS) to capture Centers for Disease Control and Prevention (CDC) contact sheet information for travelers who are at risk of coronavirus exposure based on a CDC hit or reason-for-referral notes. The PSPD Advanced Passenger Information System (APIS) team developed and deployed functionality that transmitted secondary contact phone numbers and email addresses to support CDC contact tracing efforts, as well as supporting TASPD and OFO in testing these new data elements with major commercial airlines and service providers.

Although the U.S. closed land borders early in the pandemic, there were still certain traveler types that were allowed across the border through Port of Entry's (POE), and many presented documents not compliant with Western Hemisphere Travel Initiative (WHTI) requirements. As such documents are not machine-readable, CBP officers must handle them physically, and PSPD Inspections Processing and Land Border Integration Divisions worked with local officers to develop and deploy two new solutions: an enhanced camera system that displays an image of the travel document, and a modification to the Vehicle Primary Client (VPC). These solutions together allowed officers a contactless way to not only view and enter a traveler's information into the system, but the ability to select passengers from previous system entries instead of manually handling and entering documents so that travelers and officers remain safe from COVID-19.

FY20 HIGHLIGHTS

The TDED program processed around 170,000 passports a day from the Department of State.

ESTA processed over six million VWP applications in FY2020, and collected almost $90 million in fees.

46 kiosks were upgraded at Dulles International Airport (IAD) in June, and GE Facial Recognition has been added to an average of two POEs per month

SA has been deployed to 31 air, sea, and pedestrian locations and has processed 1.4 million primary inspections since its debut.

TRUSTED TRAVELER AND INTELLIGENCE SUPPORT

Fiscal Year 2020 was a busy year for Trusted Traveler programs. FY20 also saw the implementation of projects to allow for the faster processing of travelers. For PSPD, Global Entry (GE) began rollout of its Global Entry Next Generation project, which will focus initially on facial recognition technology at ports of entry to collect a photo and accurately verify the identity of the GE member. Utilizing photo comparisons from CBP holdings that will give CBP officers the ability to conduct faster and more efficient passenger processing through CBP, and save the traveler valuable time.

TASPD also established new infrastructure processes and analytical enhancements, such as the Traveler Verification Service (TVS), a facial recognition matching solution that was initially deployed in FY16 to support OFO's congressional mandate to implement a biometric entry/exit system. The service uses cutting-edge technology in Amazon Web Services (AWS) cloud service platform to help identify travelers entering and exiting U.S., and currently is used in air, land, and sea environments with various airline and cruise line partners to install photo capture solutions. Since the initial deployment, CBP received over 50 commitment letters from airline and airport authorities, as well as letters from all major cruise lines, to outfit their respective ports with photo capture solutions that will interface with TVS. By the end of FY20, TASPD deployed TVS for use in primary processing at 18 airports, including four preclearance locations, for air exit confirmations at 20 airports, for sea processing at seven ports, and numerous land ports of entry across the southern and northern border for processing pedestrian traffic. Through the use of biometric scans, OFO has confirmed over 60,000 visa overstays and identified 289 imposters.

TASPD supported the NTC by enhancing the Unified Passenger (UPAX) vetting system to comply with over 100 User Defined Rules related to COVID-19 travel restrictions. The User Defined Rules targeted foreign individuals who are not authorized to travel to the U.S. from designated countries (China, Iran, Schengen countries, UK, Ireland, and Brazil) and facilitated travel for U.S. persons returning from these countries through funneling airports.

In support of the CDC's contact tracing efforts, TASPD implemented a new feed to the CDC to include all persons who have arrived at a U.S. Port of Entry (POE) with recent travel to a 212F country, based on travelers identified through the COVID-19 User Defined Rules. This transmission includes any available contact data, address, primary and secondary phone numbers, and email address from ATS data sources and interfaces.

TRUSTED TRAVELER AND INTELLIGENCE SUPPORT

Driven by requirements identified by CBP Intelligence Units, the Intelligence Reporting System – Next Generation (IRS NG) has expanded the core capabilities to include a collection of specialized applications to enhance CBP's threat identification and analysis as well as counter network capabilities. These specialized application support various phases of the Intelligence Cycle. With the initial deployment of the Seizure and Apprehension Workflow (SaAW) and the Threat Network Exploitation Tool (TNET) in FY19, TASPD worked with various intelligence units to ensure all respective sectors and field offices were trained on the new applications in FY20. The buy-in and quick adoption from the field helped facilitate the tracking of over 1,500 threat networks and the identification of over 30,000 members in TNET and over 43,000 interview notes created through SaAW.

In FY20, the IRS-NG team deployed numerous changes to enhance the fields ability to collect, analyze, and ultimately manage the production of informational and intelligence products disseminated across CBP and to other DHS components via the Analytical Framework for Intelligence (AFI). TASPD has worked closely with its partners to ensure the system and its products align with CBP Intelligence Enterprise doctrine to include the deployment of the Intelligence Enterprise Reports Management (IERM) and Intelligence Enterprise Product Management (IEPM) modules. These new modules will assist our Intelligence partners in tracking their Unclassified and Classified products and generated reports.

FY20 HIGHLIGHTS

ATS-G deployed in four new countries in FY2020

Provided system upgrades for 14 countries

TASPD developed and deployed web services to submit biometric requests to Hellenic Police (Greece) from DHS stakeholders through SRTP.

GTAS deployed in six new countries in FY2020, including Pakistan

GTAS is the first Foreign Partner Air Passenger Application to be deployed in the Cloud

TASPD also provides solutions that support CBP inspection and enforcement activities. The directorate is responsible for improving, administering, and maintaining selectivity and targeting systems to help secure the supply chain and support CBP's layered defense strategy for international cargo and passengers. TASPD also works closely with the OT, OFO, Office of Intelligence (OI), and USBP to realize greater effectiveness in combating terrorism, drug and alien smuggling, and other crimes within its jurisdiction through the development of new systems for analysis, integration, and rapid dissemination of relevant information.

Driven by requirements identified by CBP Intelligence Units, the Intelligence Reporting System – Next Generation (IRS NG) has expanded the core capabilities to include a collection of specialized applications to enhance the CBP's threat identification and analysis as well as counter network capabilities. These specialized applications support various phases of the intelligence cycle. With the initial deployment of the Seizure and Apprehension Workflow (SaAW) and the Threat Network Exploitation Tool (TNET) in FY19, TASPD worked with various intelligence units to ensure all respective sectors and field offices were trained on the new applications in FY20. The buy-in and quick adoption from the field helped facilitate the tracking of over 1,500 threat networks and the identification of over 30,000 members in TNET and over 43,000 interview notes created through SaAW.

In FY20, the IRS-NG team deployed numerous changes to enhance the fields ability to collect, analyze, and ultimately manage the production of informational and intelligence products disseminated across CBP and to other DHS components via the Analytical Framework for Intelligence (AFI). TASPD has worked closely with its partners to ensure the system and its products align with CBP Intelligence Enterprise doctrine to include the deployment of the Intelligence Enterprise Reports Management (IERM) and Intelligence Enterprise Product Management (IEPM) modules. These new modules will assist our Intelligence partners in tracking their Unclassified and Classified products and generated reports.

INTERNATIONAL COORDINATION

International coordination is a critical element in the success of TASPD; among other targeting missions, the directorate provides CBP and international partners with the systems, upgrades, and enhancements to analyze and evaluate traveler information as a means of combating transnational crime and other threats to national security. The programs consist of the Automated Targeting System – Global (ATS-G), Foreign Encounters, and Global Travel Assessment System (GTAS).

Automated Targeting System - Global (ATS-G) is a real-time passenger screening system. The ATS-G application evaluates passengers and crewmembers to assist foreign partner government officials in the decision-making process about whether an individual should receive additional screening prior to travel. TASPD expanded CBP's international footprint and its partnerships this year by successfully deploying ATS-G to four new countries. The four new deployments increased CBP's information sharing posture and cooperative relationship with foreign countries, particularly to mitigate risks associated with criminal and terrorist exploitation of international travel.

FY20 HIGHLIGHTS

ATS-G deployed in four new countries in FY2020

Provided system upgrades for 14 countries

INTERNATIONAL COORDINATION

Foreign Encounters consists of four programs that collect biometric and biographic data on subjects encountered abroad. Foreign Encounters collects its data from international programs, including the Biometric Data Sharing Program (BDSP), Biometric Identification Transnational Migration Alert Program (BITMAP), Secure Real-Time Transport Protocol Version 2 (SRTP v2), and Foreign Border Crossing Records (FBCR). These data collections on subjects of interest for Foreign Service Law Enforcement Agencies use automated biometric and biographic data sharing capabilities, and a formalized, fully compliant, scalable, and centralized biometric data analytical enterprise that is fully interoperable between the partnering stakeholders. These four programs, combined with Foreign APIS data, provide an interactive hotlist to DHS users for collaboration on subjects of interest encountered by Foreign Partners.

On July 5, 2017, CBP formed a partnership with the World Customs Organization for the distribution of GTAS - an open source passenger screening solution available for foreign entities or government partners to adopt to encourage international passenger data sharing. To date, eight countries have agreed to partner with the U.S. and use GTAS. This DHS flagship open government initiative has become a valuable testbed for nascent technology, innovative ideas, and cloud deployment strategy. GTAS compliments the United States' approach for foreign partner engagement in air passenger security, opens new doors for interagency support and communication in support of the mission, while providing a direct avenue for countries to comply with United Nations Security Council Resolutions 2178 and 2396.

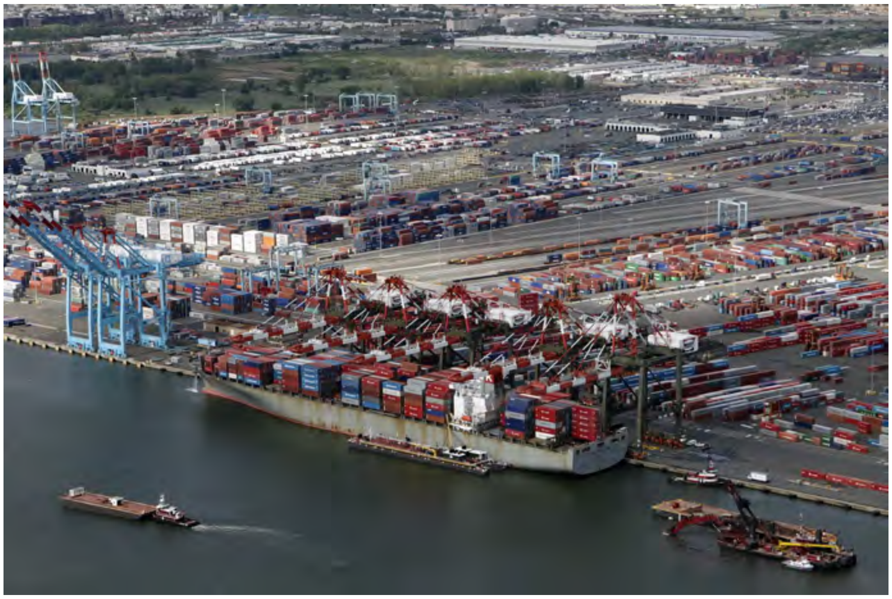
FY20 HIGHLIGHTS

TASPD developed and deployed web services to submit biometric requests to Hellenic Police (Greece) from DHS stakeholders through SRTP.

GTAS deployed in six new countries in FY2020, including Pakistan

GTAS is the first Foreign Partner Air Passenger application to be deployed in the cloud

TRADE FACILITATION



Cargo Systems Program Directorate (CSPD) continues to modernize and enhance applications in the cloud, creating a more resilient and reliable system without negative impact to the end user. Through the cloud environment, CSPD bolsters the system's security, increases automation reducing risk of human error, realizes benefits streamlined collection processes, and improves accountability while improving lawful international trade.

In July, the Technology Modernization Fund (TMF) awarded $15 million to CBP to modernize the 30-year-old collection tool, the Automated Commercial System (ACS), the last remaining mainframe solution for the agency. The TMF award will help fund the migration of the remaining collections modules off the legacy mainframe and the into cloud, thereby increasing resiliency and reliability of CBP's financial system and enabling the essential flow of international trade.

The new Truck Manifest Trade Facing User Interface launched in summer 2020. The new Truck Manifest is housed in the CBP Cloud. Continued modernization to Truck Manifest will include updates for primary and secondary processing.

New Cloud Native, also known as New ACE, applications deployed in FY20 to include AD/CVD, Truck Manifest User Interface, Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA) Risk-Based Bonding and Mass Processing, Type 86 enhancements. All current and future enhancements are built from the ground up with resiliency and monitoring in mind.

CSPD coordinated closely with the OT and the U.S. Trade Representative to implement President Trump's Executive Order initiating a 90 calendar day payment deferral for the deposit of certain estimated duties, taxes, and fees for importers experiencing a significant financial hardship due to COVID-19. CSPD used a Robotic Process Automation bot – to increase efficiency and decrease the staff workload on this effort.

In support of the OT mission, the ATAP will provide OT a single, organized point of access for all of CBP's internal and external sources of information, enhanced predictive and prescriptive analytic capabilities, a unified case management system that allows for OT enterprise collaboration and data sharing between offices and power visualization capabilities utilizing the single source of data. ATAP will establish a service delivery model to allow OT to develop customized solutions for the unique trade analytics questions presented to CBP on a frequent basis.

TRADE FACILITATION

In late September 2019, CSPD coordinated with OT to implement the Entry Type 86 commercial entry process in response to the increase in Section 321, Type 86 *de minimis* import entries. These import entries are worth under $800 in value in the country of origin and are admitted to the U.S. duty and tax free. Entry Type 86 allows customs brokers and self-filers to submit electronic *de minimis* entries through Automated Broker Interface (ABI), including those subject to Participating Government Agency (PGA) data requirements for clearance. Entry Type 86 helps CBP manage the flow of goods, creating greater visibility for low-value shipments entering the U.S. while improving border protection, import security, and safety. Although participation is voluntary, Type 86 entries have surpassed 88 million.

In coordination with OT, CSPD teams continue to implement high priority and quick turnaround enhanced capabilities in ACE to support presidentially mandated actions including Section 232, Section 301, and International Economic Emergency Powers Act (IEEPA) updates. These coordinated updates occur on a regular basis.

CSPD representatives engaged OT/ TTO to plan and implement the U.S.-Mexico-Canada Trade Agreement (USMCA) where topics included timing of the legislation, duty elimination, country of origin/export rules, tariff preference levels (TPLs), and merchandise processing fee requirements. Additional automobile importation topics included ACE support of tracking data for the Department of Labor's enforcement of the 'wage' requirement, and the Office of the U.S. Trade Representative's enforcement of the 'North American steel and aluminum content' requirement.

Trade Remedies are actions taken in response to subsidies, sales at less than fair value, and import surges. Starting in May 2018, the ACE system has supported efforts by the Office of the U.S. Trade Representative to enforce various enhanced trade remedy measures.

Here are some measures and examples:

- Safeguard National Security
- Steel and Aluminum products
- Protect Domestic Industry
- Washing Machine & Solar Panel products
- Target International Trade Violators
- Products from China & the European Union (EU)

In order to enforce the laws of our nation, OT/CSPD has been in direct contact with the White House on an ad hoc basis and worked tirelessly to develop code to enact trade remedies in an immediate fashion. The configurable nature of ACE's design allows CSPD to prepare for last minute decisions regarding the activation of high-profile presidential proclamation trade actions.

FY20 HIGHLIGHTS

In FY20, deployed New ACE cloud applications, including Truck Manifest User Interface, and Type 86 enhancements.

Launched new Truck Manifest Trade facing User Interface via the cloud with planned primary and secondary processing modernization.

NETWORK RESILIENCY

In FY20, OIT continued to improve the resiliency capabilities of CBP's network infrastructure, ensuring high-performing connectivity and access to mission-enabling technologies. OIT directorates collaborated to guarantee CBP employees have the high performing, always available network necessary to execute their mission and continue operations uncompromised in the face of a disaster or attack.

Enterprise Network and Technology Support (ENTSD), tasked with delivering resilient and reliable technology systems, tools, and services, moved OIT toward a more secure and robust network. ENTSD invested in rapid and dependable connectivity by improving network performance at over 530 sites with circuit upgrades, refreshed switches, and 4G backup installations. ENTSD developed visualization dashboards to boost network monitoring, created automated network support checklists to improve incident resolution speed, and completed over 130 domestic and international site visits to ensure the resiliency and reliability of field equipment.

NETWORK RESILIENCY

ENTSD successfully initialized a network automation practice that converts manual steps into a highly-repeatable 30-second process for applications like the Automated Commercial Environment (ACE), Automated Passport Control (APC), Automated Targeting System (ATS), Traveler Primary Arrival Client (TPAC), Secure Flight (SF), Amazon Web Services (AWS) US-East Environment (CACE), Food and Drug Administration (FDA) Secure File Transfer Protocol (SFTP) Virtual Private Network (VPN), Mainframe as a Service (MFaaS), Microsoft Office O365 Email Service, TECS, E3, and Global Protect VPN. The network automation practice removes human error, increases productivity, improves consistency of key processes, reduces network operation complexity and lowers cost.. ENTSD's improvements in network resiliency will help ensure ENTSD can rapidly react, respond, and minimize the impact of possible outages, disruptions, or attacks.

The Enterprise Data Management and Engineering Directorate (EDMED) was another key partner in the agency-wide push for greater resiliency and recovery capabilities for both network and physical infrastructure. In FY20, EDMED, the OIT infrastructure and operations division, led a power upgrade in CBP's National Data Center 1 (NDC1) that gave the data center the capability to function without interruption upon the loss of power at any level. This effort included shutting down Legacy Uninterruptible Power Supplies (UPS) A, shutting down of UPS B, connecting the new Legacy power feeds to seven Power Distribution Units (PDU), and, finally, bringing Mission Critical Support Platform power to the legacy side and allowing the old panels to be removed from UPS A. For the first time ever, CBP achieved 100% redundancy for its PDU equipment at NDC1, which will now recover faster from power disruptions, power outages or power failure.

ENTSD and EDMED, collaborated to enable enterprise cloud service and successfully implemented an Amazon Web Service Transit Gateway. The transit gateway, a central hub that scales elastically based on changing application traffic patterns, allows CBP to consolidate different AWS accounts VPCs and network connections. Along with upgraded cloud circuit capacity to meet projected growth demands, OIT now also has the ability to meet unexpected demands for cloud services and eliminates single points of failures in order to support mission partner experiences and needs.

FY20 HIGHLIGHTS

Increased network speed and resiliency for 530+ circuits at USBP, OFO, and AMO sites by upgrading circuits, refreshing switches, and installing 4G backups

100% redundancy for equipment at NDC1, by enhancing reliability from two power feeds at both ends of the facility

Deployed over 130 TDYs and completed ~90 site visits to execute priority requests and ensure continued equipment resiliency and reliability

Implemented a stable and resilient Remote Access VPN solution for CBP's teleworking workforce and faster connections to 70,000+ Office 365 users

Implemented a cloud-based threat detection and mitigation solution to protect the CBP network and its workforce from distributed denial-of-service (DDOS) attacks

CLOUD MIGRATION

CBP is in the midst of modernizing fundamental IT operations by migrating its infrastructure to cloud. A primary factor for cloud migration is improving the mission experience. OIT understands the mission customer must have fast, reliable, secure, and tactical support to conduct day-to-day operations. From a mission perspective, cloud-based technology will improve availability of CBP applications, connectivity, and data processing, which directly benefits our frontline agents and officers. From an operational perspective, cloud will enable automation, self-service, and improve technology business management. All of these benefits combine to help OIT provide the support that our mission partners rely on every day.

Cloud migration is a team effort and requires modernization in all parts of the application development, deployment, and sustainment lifecycle. Over the last year, OIT's application teams have continued modernizing application architecture through refactoring, containerization, and cloud native development practices to take advantage of cloud-enabled features for ideal application performance. OIT's infrastructure teams continue to develop cloud-based environments to host applications in a secure and resilient manner. OIT's enabling teams are supporting innovation in the way we reimagine service delivery and improve our customer's experience.

Due to OIT's continuous investments in modernization and innovation for cloud initiatives, OIT easily adjusted to higher demands in a telework environment and provided access to heightened cloud needs brought on by COVID-19. OIT successfully ramped up virtual training efforts for O365 capabilities, especially for MS Teams, to make sure all 60,000+ CBP employees had access to cloud applications to provide uninterrupted services to CBP partners for continuation of mission operations. To enhance knowledge management in a virtual environment, OIT conducted 63 training workshops and augmented the O365 website by creating informational sections and frequently asked questions (FAQs) for every O365 app currently available. OIT even deployed AWS1, Kubernetes, and Splunk to increase versatility for CBP's multi-cloud environment approach, and launched ServiceNow to enable automation for its help desk ticket management system.

CLOUD MIGRATION

In FY20, CBP exceeded its targets for cloud migration. OIT's Data Center and Cloud efforts delivered key initiatives around security, resiliency, modernization, adoption, and development to enhance experiences across the enterprise.

To increase security capabilities, OIT developed common control packages which enable applications that have system components across multiple cloud infrastructure environments to reuse security standards and controls. The common control packages ultimately reduced the time required to achieve an Authority to Operate (ATO) down to four to six months. The OIT Cybersecurity team worked through several major application and general support system ATOs required for cloud applications and services, and approved 13 ATOs for new services and systems, while maintaining security compliance for systems with existing ATOs through continuous monitoring activities.

To bolster resiliency of cloud services, OIT simplified operations across the agency to provide application teams with highly available and redundant, hybrid and multi-cloud environments to support mission critical applications. OIT upgraded its data center power to operate seamlessly across CBP’s hybrid environment and recover critical services faster from power disruptions, outages, or failure.

Furthermore, CBP deployed an AWS Transit Gateway that consolidates different AWS accounts, VPCs and on-premise network connections in a centralized hub. This capability provides OIT key benefits, such as easily meeting unexpected demands for cloud applications and eliminating single point of failure or bandwidth bottlenecks for delivering cloud services.

To modernize infrastructure, OIT migrated all equipment out of Data Center 2 (DC2) ahead of the DHS mandated deadline of June 2020. Mission-critical systems such as TECS Disaster Recovery (DR) were migrated to the cloud as a part of this larger effort. This resulted in the reduction of costly hosting fees by migrating to either a pre-existing infrastructure at the National Data Center (NDC) or to a more cost-effective cloud-based service provider.

To enhance application development, OIT deployed its new cloud enterprise offering, Kubernetes Containerization Platform. Kubernetes helps OIT leverage existing cloud investments while supporting the DevSecOps model of architecture. This enables CBP to continue moving forward in the cloud application modernization methodologies while providing essential building blocks for all CBP development teams to leverage the reuse of platform(s) and move quickly to meet ever-changing mission priorities.

FY20 HIGHLIGHTS

Deployed **30%** (91 applications) of CBP’s total application portfolio to **eight accredited cloud environments**

Deployed a COVID Workforce Incident Tracker to over **60,000** CBP employees in Salesforce

Onboarded **41** projects to the CBP Amazon Cloud East (CACE) environment and saved **almost two million dollars** through cost optimizations

Delivered a successful demonstration of enterprise data hub capabilities in a cloud environment, **(95% faster)** and lower costs **(70% less expensive)**

Enabled emerging **technology pilots** in Artificial Intelligence, Robotics Process Automation, Machine Learning, and Data Management

CYBERSECURITY

The Cyber Security Directorate (CSD) proactively manages cybersecurity risks, coordinates cyber information sharing, and provides an agile, effective, and cost-efficient approach to cybersecurity that aligns to the evolving cyber threat environment. CSD envisions a mature cyber program that secures CBP's technology assets and protects the mission by implementing proactive, risk-based cybersecurity practices to create a strong and resilient security posture and workforce.

This fiscal year, CSD worked to significantly mature CBP's security program by implementing new technology, creating and updating processes and procedures, and optimizing operations. As a result of DHS's first ever 100% remote Cybersecurity Service Provider (CSP) evaluation, CBP is authorized to be a CSP Center of Excellence. CSD helped to achieve this mark by rapidly maturing the OIT cybersecurity program to include the critical CSP functions of cyber incident response, attack sensing and warning, warning intelligence collection and correlation, insider threat monitoring, malware protection, vulnerability management, and cyber risk assessments. As an authorized DHS CSP, CBP can offer its security services to other DHS components.

CSD established its Project Management Office (PMO) to provide an enterprise-wide approach to identify and prioritize security initiatives and projects that align with the directorate's mission and strategic goals. This technology portfolio created a foundation for the enhanced awareness and collaboration, increased efficiency, and more consistent delivery of the right projects at the right time with the right resources. One of the PMO's successful FY20 projects was integration with DHS's Swimlane capability to reduce the time to respond and apply higher critical thinking to contain and remediate threats. This integration greatly improves security incident and event management triage in responding to phishing attacks and threat intelligence. As a result, OIT reduced the processing time of phishing email tasks by 95% from 42 to 2.5 minutes per task, which allowed CSD cyber analysts to be more productive in other areas. To collect intelligence from all sources on nation-state cyber threats and associated tactics, techniques and procedures, CSD developed and implemented an advanced persistent threat (APT) profiling matrix. CSD uses the threat matrix to develop content for weekly cyber threat intelligence briefings for OIT executive leadership, raising awareness of active adversarial campaigns including cyber-criminals, hacktivists, and nation-state funded APTs that pose a threat to CBP users, networks, infrastructure and operations. This intelligence is also used to conduct structure threat assessments against CBP systems and high value assets to ascertain security posture and exposure.

CYBERSECURITY

CSD built an integrated SailPoint/ CyberArk platform to create a workflow-driven zero-trust environment supporting privileged users to protect critical infrastructures. CSD also developed a tool to ensure access management to critical CBP applications for DHS, other government agencies, trade partners, and the public sector. The directorate deployed Splunk to CBP's cloud environment to ingest and monitor log data across CBP's cloud environment and further reduce our on-premise instance. Splunk provides the IT security team actionable insight into what a user is doing, if that user is allowed to do it, and how much the user's actions stray from the norm. Deploying Splunk Universal Forwarder to all CBP user workstations and laptops provides an automated mechanism to facilitate secure data collection logs from these types of devices. Through the use of Splunk Enterprise Security as well as other Splunk monitoring and reporting applications, the CBP Security Operations Center has a greater level of visibility into the events that occur within these types of devices. With this enhanced level of visibility, the SOC can take a more proactive approach to the identification, investigation, and mitigation of potential malicious actions before wider proliferation can occur.

To support CBP's requirement to attract and retain cybersecurity professionals, CSD established the Information System Security Officer (ISSO) Bench. ISSOs are charged with ensuring maintenance of the proper operational security posture for an information system. The ISSO Bench provides system security services, on an as needed basis, throughout OIT, and provides additional system security and assessment support, evaluate external information systems for control responsibility, and provides training sessions to the ISSO community.

CBP STRATEGIC PLAN

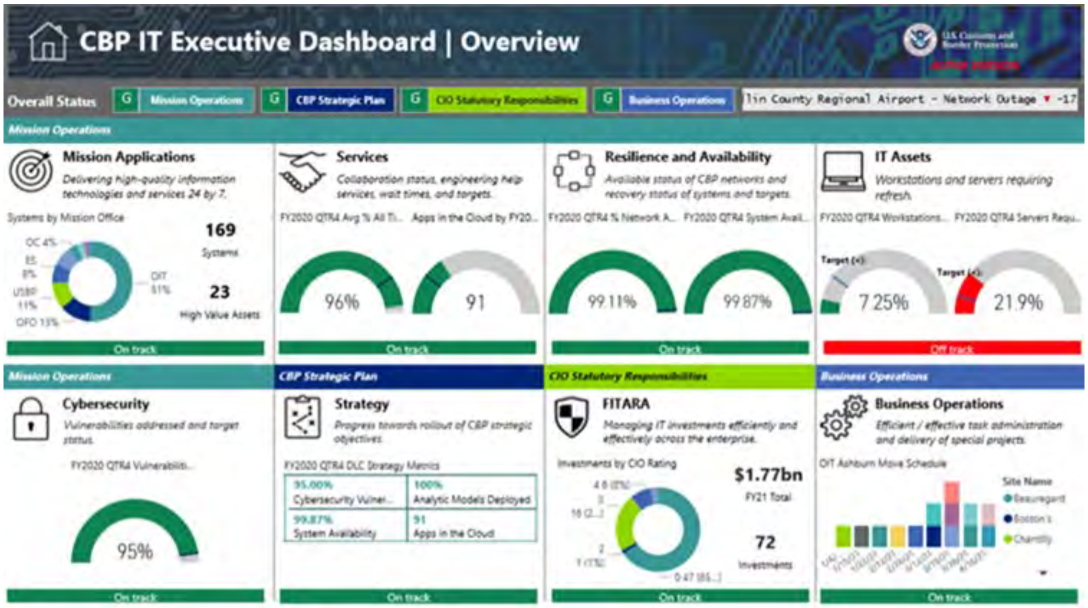
INFORMATION AND TECHNOLOGY EXECUTIVE MANAGEMENT DASHBOARD

The IT Executive Management Dashboard (EMD) previously known as the CIO Dashboard, is a leadership-focused dashboard that enables OIT's Assistant Commissioner, Deputy Assistant Commissioner, Executive Directors and Directors to manage and govern OIT's strategy and program management implementation in alignment to mission operations. It will provide transparency to OIT leadership, facilitate rapid responses, and provide situational awareness to meet evolving mission priorities. The OIT-EMD will be a single source of information to support executive leadership in the collective management of OIT.

The OIT-EMD will:

- deliver OIT Governance and program management in a light weight and easily consumed manner;
- improve the ability to measure, monitor, and manage progress against Strategic Objectives;
- create on-demand, self-service insights into performance management and increased mission effectiveness;
- provide centralized information which allows users to drill-through activities and performance tied to OIT & CBP mission needs; and
- allow for a broader understanding and deeper insights into the performance of OIT systems and program.

The development of the dashboard will take place in two phases. In phase one, the development team will coordinate with data owners to access data, understand appropriate use of metrics for reporting purposes, and establish direct connections between the CIO Dashboard and available datasets. The dashboard development team to obtain the necessary data for the dashboard, to show correct and complete data sets through the CIO Dashboard. The first phase of data gathering will take place in October. In the second phase, the data team will secure access to full datasets of existing OIT dashboards to allow the creation of new visualizations and metrics within the CIO Dashboard. The goal is to have the CIO Dashboard fully operational by February 2021.



CBP IT Executive Dashboard | Overview

Overall Status: G Mission Operations | G CBP Strategic Plan | G CIO Statutory Responsibilities | G Business Operations | lin County Regional Airport - Network Outage ▼ -17

Mission Operations

Mission Applications — Delivering high-quality information technologies and services 24 by 7.

Services — Collaboration status, engineering help services, wait times, and targets.

Resilience and Availability — Available status of CBP networks and recovery status of systems and targets.

IT Assets — Workstations and servers requiring refresh.

Mission Operations

Cybersecurity — Vulnerabilities addressed and target status.

CBP Strategic Plan

Strategy — Progress towards rollout of CBP strategic objectives.

FY2020 QTR4 DLC Strategy Metrics

95.00% Cybersecurity Vulner...	100% Analytic Models Deployed
99.87% System Availability	91 Apps in the Cloud

CIO Statutory Responsibilities

FITARA — Managing IT investments efficiently and effectively across the enterprise.

Business Operations

Business Operations — Efficient / effective task administration and delivery of special projects.

U.S. Customs and Border Protection
ALPHA VERSION
Systems by Mission Office
OC 4%
ES 8%
USBP 11%
OFO 13%
OIT 51%
169
Systems
23
High Value Assets
On track
FY2020 QTR4 Avg % All Ti...
Apps in the Cloud by FY20...
96%
91
On track
FY2020 QTR4 % Network A...
FY2020 QTR4 System Avail...
99.11%
99.87%
On track
FY2020 QTR4 Workstations...
FY2020 QTR4 Servers Requ...
Target (<)
Target (<)
7.25%
21.9%
Off track
FY2020 QTR4 Vulnerabiliti...
95%
On track
On track
Investments by CIO Rating
4.6 (6%)
3
16 (2...)
2
1 (1%)
0.47 (65...)
$1.77bn
FY21 Total
72
Investments
On track
OIT Ashburn Move Schedule
Site Name
Beauregard
Boston's
Chantilly
On track

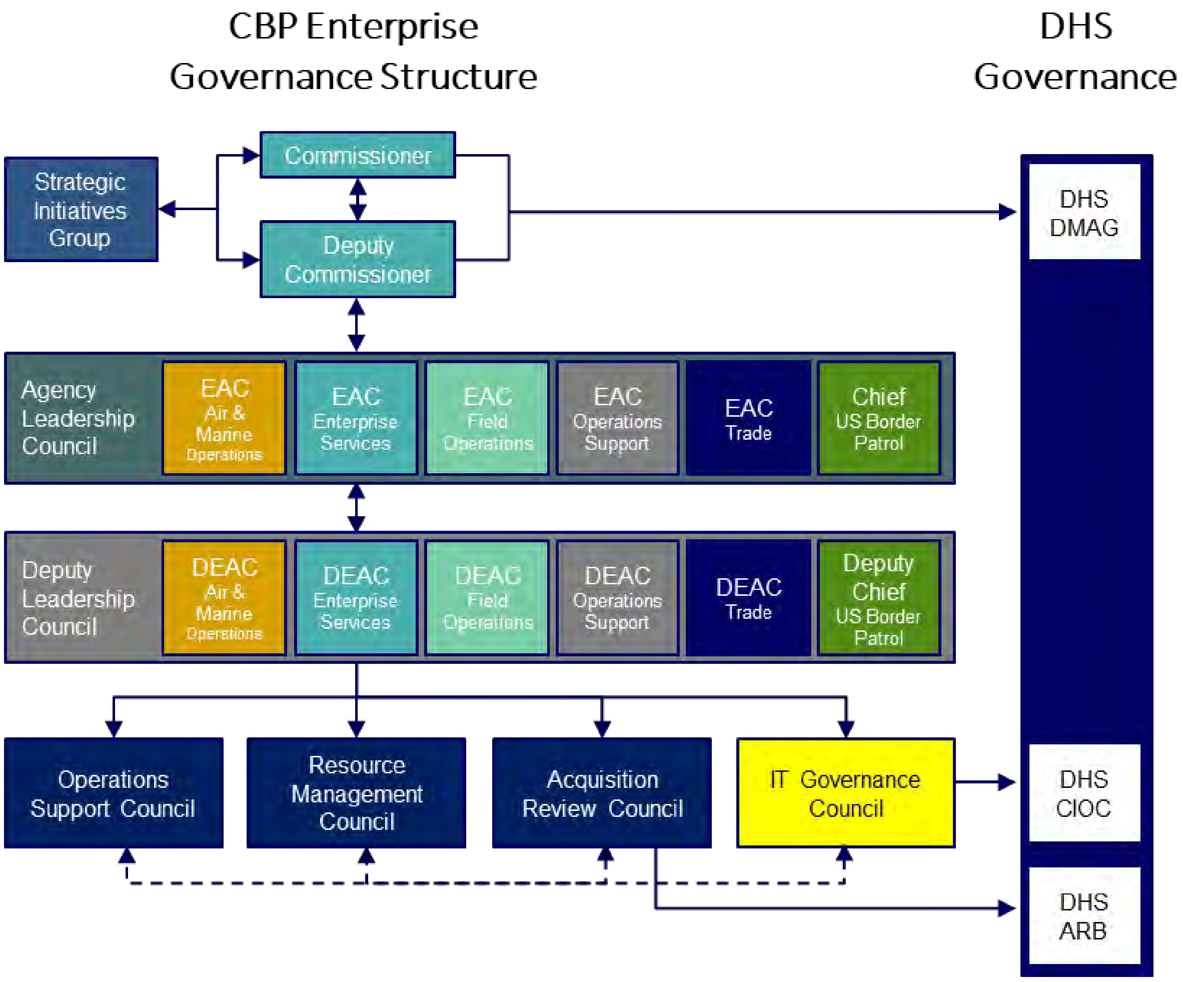
*FITARA-$1.77B represents CBPs IT and IT/mixed Investments as reported in INVEST

STATUTORY RESPONSIBILITIES

INFORMATION TECHNOLOGY GOVERNANCE COUNCIL

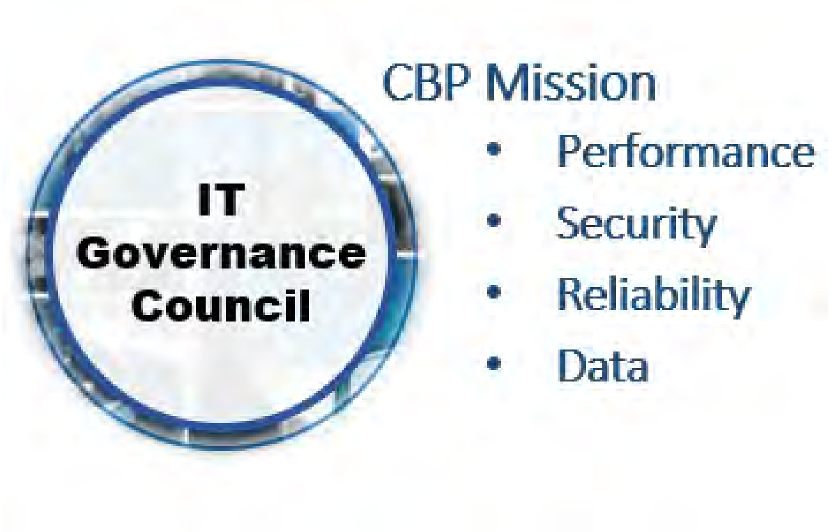
OIT, along with the Commissioner's Office, has proposed the establishment of the IT Governance Council (ITGC), a forum for leaders from CBP to set priorities and to provide governance for the CBP Information Technology/ Information Resource Management (IT/IRM) enterprise. ITGC a key element of CBP's corporate governance structure.

Similar in nature to the Resource Management Council, the Acquisition Review Council (ARC), and the Operations Support Council (OSC), the ITGC will be an enterprise wide body that represents the interests, requirements, and preferences of all CBP mission offices. Specifically, the ITGC: provides oversight and direction in the implementation of the Agency's Information Technology (IT)/ Information Resource Management (IRM) investments, including, but not limited to decisions related to Cybersecurity, Enterprise Architecture and technology standards, and all aspects of data and records management; supports strategy and vision to provide transparent, responsive, and accountable IT/IRM investments across Mission Offices in support of the CBP user community; provides leadership, guidance, and operational direction to subordinate CBP IT/IRM Governance boards (e.g. Technology Review Board, IT Financial Review Board);
and makes recommendations for future IT/IRM investments to the Resource Management Council (RMC) and the Deputies Leadership Council (DLC).


CBP Enterprise Governance Structure
DHS Governance
Strategic Initiatives Group
Commissioner
Deputy Commissioner
DHS DMAG
Agency Leadership Council
EAC Air & Marine Operations
EAC Enterprise Services
EAC Field Operations
EAC Operations Support
EAC Trade
Chief US Border Patrol
Deputy Leadership Council
DEAC Air & Marine Operations
DEAC Enterprise Services
DEAC Field Operations
DEAC Operations Support
DEAC Trade
Deputy Chief US Border Patrol
Operations Support Council
Resource Management Council
Acquisition Review Council
IT Governance Council
DHS CIOC
DHS ARB

INFORMATION TECHNOLOGY GOVERNANCE COUNCIL

The Information Technology Governance Council (IGCE) will reinforce the three values outlined in the guiding principles in the CBP OIT Strategic Plan. First, the council values collaboration; OIT works best when its components work together, partner with its customers, industry, and across the CBP enterprise to share insights, spur innovation and collectively meet mission challenges. The second value is mission focus. OIT strives to increase its individual and collective understanding of the mission needs of frontline and mission support personnel, proactively helping them understand how technology can support their needs. The third value is resilience. OIT embraces the notion that change is constant. As mission needs and technologies evolve, OIT will adapt its approaches to deliver mission value through modern, secure, resilient, and scalable technologies and methods.



IT Governance Council

CBP Mission

- Performance
- Security
- Reliability
- Data

HIGHLIGHTS

CIO/CAE coordination to enhance IT Acquisition Governance by recommending the establishment of an OIT Portfolio Acquisition Executive who oversees and directs the Enterprise Services Acquisition Portfolio Management Directorate

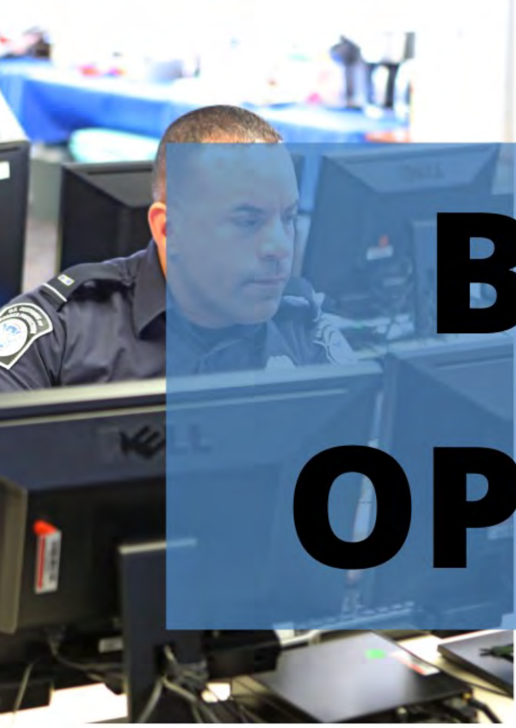
95 FY20 acquisition document reviews

Identified and addressed IT/IRM issues early in the lifecycle

Cost Wise Readiness optimizes use of resources for maintenance

Increased collaboration with OA and CHENG on SELC reviews

Technology Review Board (TRB) establishment



BUSINESS OPERATIONS

ASHBURN/REINTEGRATION

CBP has signed an Occupancy Agreement with the General Services Administration (GSA) for a new facility in Ashburn, VA that will consolidate 85% of the agency's Northern Virginia locations onto one campus. This consolidation affects not only OIT, but also U.S. Border Patrol's Tactical Air, Land and Marine Enterprise Communications, Operation Services Laboratory and Scientific Services Division and Office of Trade's Trade and Transformation Office. CBP has decided to retain a few existing locations for flexibility and project completion to better align with cloud migration funding that is anticipated, CBP has decided to extend the lease of NDC(1) to provide additional time for cloud migration to be completed.

FY20 was an exciting time for the Ashburn Project. The Office of Facilities and Asset Management (OFAM) is the lead component, and as the year ended, construction work was just about completed and furniture installations well underway. As the 2020 calendar year comes to a close, OFAM is managing final procurements for audio visual and infrastructure pieces. Through the lens of the COVID Pandemic, employees are planning to move in FY2021 when it is safe to do so.

The Ashburn office space offers a number of modern features and amenities including the following:

- Numerous conference rooms with room dividers that allows for expansion or contraction based on occupants need;
- Break rooms, kitchenettes and collaboration spaces throughout the building;
- Onsite cafeteria and coffee shop;
- A number of special use spaces including an Innovation Room, state of the art Enterprise Operations Center, spacious Security Operations Center, and IT testing laboratories;
- A large conference and training center with retractable walls where special events, all hands meetings and training courses can be conducted;
- Modern architecture and bright and open areas;
- Efficient multi-functional devices for printing and faxing and soft phones integrated with Office 365; and,
- A number of restaurants, retail stores, gyms and other amenities are located within a few miles of the campus.

While the team continues to build out the space, the health and well-being of all OIT staff members remains a top priority. OIT leadership is continually working with OFAM's Project Team to monitor pending current and post-COVID norms and guidelines to ensure all buildings are compliant in every aspect. After many months of planning and construction, we look forward to occupying the thoughtfully designed offices at Ashburn.

PARTNERSHIPS

TRUSTED PARTNER INITIATIVE

OIT Trusted Partnerships

The Trusted Partnership engagement strategically supports CBP mission success.

Quarterly interactions provide insight into CBP mission needs, provide transparency to the Trusted Partner, and informs OIT on how to invest resources to better support mission success.

Partnership Objectives:

Integration & Transparency

Increase IT initiative integration and transparency within CBP mission offices and enterprise support organizations

Governance

Establish CBP IT governance structure with Mission Offices to meet agency and DHS guidance

Data-Driven Decision Making

Meet with IT stakeholders on a quarterly basis to provide business intelligence insights and optimize resource allocation

Achieved through....

QUARTERLY IN DEPTH REVIEW

PERIODIC TOUCH BASE

DASHBOARDS

CBP BORDER 5/MIGRATION 5

The CIO Technology Forum is a subset of the Border/ Migration 5 initiative which works to further cooperation on border and immigration technology issues among the Five Eye countries: Australia, Canada, New Zealand, United Kingdom, and United States.

Under the leadership of the CBP OIT Assistant Commissioner, the United States chaired the B5/M5 CIO Technology Forum throughout FY2020, providing valuable leadership for the forum in identifying common opportunities for collaboration and establishing an international working group to explore opportunities to standardize and exchange specific immigration data sets. The forum successfully integrated immigration counterparts, established standardized communications, set a regular cadence of meetings, and identified projects on which countries can coordinate their efforts.

Under OIT's chairmanship, partners agreed to pursue a four-pronged strategy in which they will share information around efforts to combat COVID-19, upgrade to Secure Real Time Transfer Protocol (SRTP) version 2, migrate all of the B5/M5 partners to the Homeland Security Information Network (HSIN), and establish an integrated B5 Single Window platform. The adoption of SRTP 2 and enrollment into the HSIN will enable partners to more securely access and share sensitive information vital to international border security efforts.

OIT hosted international partners in December 2019 for the biannual in-person meeting. Attendees from the four partner countries toured CBP facilities over three days at Dulles Airport, the Ronald Reagan Building, and the National Data Center in Springfield, VA. During the three day in-person meeting, partners discussed cybersecurity, emerging technologies, and cloud migration. Partners agreed to focus on sharing best practices in these three areas, harness the work done by others on emerging technologies, and explore creating mutually acceptable standards for cloud migration, storage, and sharing.

OIT successfully transferred chairmanship of the forum to New Zealand in September 2020.

LOOKING AHEAD FY 2021

LOOKING AHEAD FY2021

With the start of FY21 and a new calendar year approaching, OIT is focused on a number of key initiatives and strategic investments that will equip the agency for continued mission success in our ever changing landscape.

CBP's 5 Enduring Mission Priorities are a central tenet to how OIT will move forward in partnership to provide service and support for mission partners across the agency in FY21. We recognize that integration, transparency and rapid response to mission needs are key to driving unified IT impact across the organization and its mission spaces.

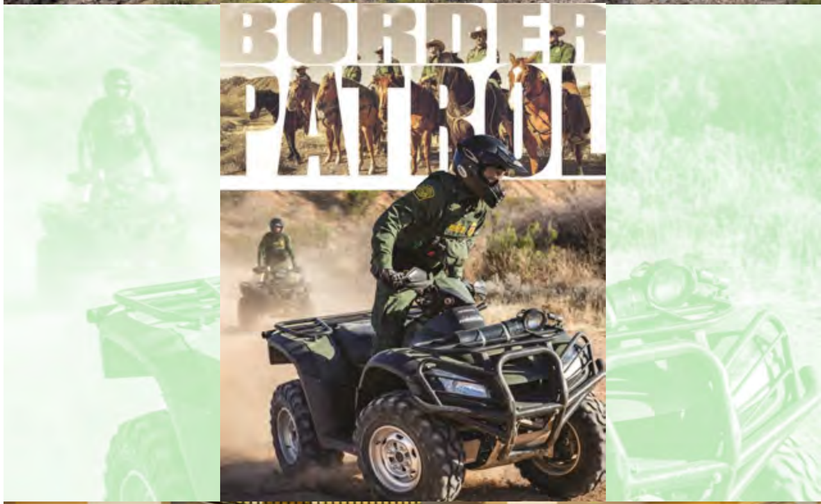
OIT is leading IT modernization efforts across the agency including increased reliance on leading industry vendors like Amazon Web Services, Google Cloud Platform, O365, Salesforce, and ServiceNow. Our ability to provide modernized IT service management and business management services will continue to mature as our portfolio footprint shifts to cloud-based infrastructure. These efforts will continue to bolster resiliency, strengthen cybersecurity, and expedite innovative deployments for our frontline mission partners.

Data Management and Analytics, including the use of Artificial Intelligence (AI) and Machine Learning (ML), will continue to play an expanded role in how OIT facilitates data to support mission critical functions, real-time landscape awareness, and proactive decision making. Further, using Robotics Process Automation (RPA) will alleviate our administrative burden and reduce reliance on manual processing time. Improving our access and use of critical information will help us bring impact to mission faster and more effectively.

OIT will utilize cutting edge technologies in FY21 to support ongoing innovations that keep pace with evolving mission needs. For instance, emerging global trends (i.e., 5G connectivity, foldable devices) may influence our mission and trade partners in areas that may transform tactical communication capabilities. We look forward to supporting increased connectivity in the field and increasing network capacity to deliver mission data to end users.

These areas of focus, along with the solid FY20 accomplishments outlined in the document above, continue to showcase CBP OIT's leadership in the federal technology space. We are committed to continued improvement and look forward to working with you in FY21.

OIT: SUPPORTING CBP AT THE SPEED OF OPERATIONS



U.S. Customs and
Border Protection