



CBP'S MISSION:
*Protect the American people, safeguard our borders,
and enhance the Nation's economic prosperity*



CBP IT STRATEGY 2023 - 2027

MESSAGE FROM THE CHIEF INFORMATION OFFICER



I am pleased to present the U.S. Customs and Border Protection (CBP) Information Technology (IT) Strategy FY2023 - 2027. As the largest IT organization in the Department of Homeland Security (DHS), with an IT budget of \$1.8 billion, CBP's Office of Information and Technology (OIT) plays a vital role in protecting and supporting our national security and prosperity. Each year, our responsibility and role as CBP OIT continues to expand. The objective of this strategy is to refresh our alignment and execution in support of our vision and mission.

Our goals for this multi-year strategy are focused on six areas: Mission Infrastructure, Mission Applications, Trusted Partners, Cybersecurity, Enterprise IT Governance, and CIO Business Operations. OIT will continue to utilize cutting edge technologies from 2023 to 2027 to support ongoing innovations that keep pace with evolving mission needs. Some of our impactful accomplishments are highlighted below:

The IT Executive Dashboard, a leadership focused dashboard, provides IT transparency to CBP leadership, facilitates rapid responses, and increases situational awareness to meet evolving mission priorities.



The Cybersecurity Strategy for FY22 – FY24 evolves and improves cybersecurity posture through defending mission operations, improving threat detection and response capabilities, shifting CBP cyber protection from primarily perimeter-facing into Zero Trust Architecture, and involving all CBP in cybersecurity Governance, Risk Management, and Compliance (GRC).



The Unified Immigration Portal (UIP) delivers mission impact to users across the immigration ecosystem through the addition of net new data sets, deployments of operational dashboards, and expansion of UIP services. These capabilities enable users, from frontline operators to senior executives to have visibility into interagency operations and improve insights for better coordination.



CBP 24/7 Mission

In advancing our strategic goals, the impact of our collective efforts amplifies across all focus areas.

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


Sincerely,

Sanjeev (Sonny) Bhagowalia
Assistant Commissioner (AC)
Office of Information & Technology (OIT)
CBP Chief Information Officer (CIO)

TABLE OF CONTENTS

PAGE #

INTRODUCTION		I. Organizational Overview II. Strategic Alignment III. Operating Environment IV. Vision and Mission V. OIT Values - Vision in Practice	4-14
STRATEGIC GOALS		OBJECTIVES	
	GOAL #1: MISSION INFRASTRUCTURE	Objective 1.1: Consolidated Enterprise Network Objective 1.2: Core Enterprise Cloud Computing Objective 1.3: IT Operations	15-19
	GOAL #2: MISSION APPLICATIONS	Objective 2.1: Digital Experience Objective 2.2: Enterprise Data Management Objective 2.3: Application Development Objective 2.4: Scalability	20-28
	GOAL #3: TRUSTED PARTNERS	Objective 3.1: Integration & Transparency Objective 3.2: Interagency Relationships Objective 3.3: Industry & International Partners	29-34
	GOAL #4: CYBERSECURITY	Objective 4.1: Cyber Hygiene Objective 4.2: Threat Detection & Response Objective 4.3: Cyber Protection Objective 4.4: Cybersecurity Governance, Risk Management, and Compliance	35-40
	GOAL #5: ENTERPRISE IT GOVERNANCE	Objective 5.1: Governing Policies / Processes Objective 5.2: Governance Boards Objective 5.3: Compliance Objective 5.4: Communications, Education & Coordination	41-48
	GOAL #6: CIO BUSINESS OPERATIONS	Objective 6.1: Strategy Management Objective 6.2: Cost and Budget Transparency Objective 6.3: Procurement / Acquisition Support Objective 6.4: OIT Workforce Experience Objective 6.5: Workforce Management	49-55
CONCLUSION		Measuring and Achieving Success	56

TABLE OF CONTENTS

INTRODUCTION

I. ORGANIZATIONAL OVERVIEW

U.S. Customs and Border Protection (CBP), one of the world's largest law enforcement organizations, is chartered to execute a focused multi-faceted mission:

1.) Ensuring that the United States remains safe from potential threats by enforcing the nation's border regulations, and 2.) Facilitating lawful international trade and travel. This mission requires CBP to serve as America's frontline and demands that all members of the organization serve the nation with vigilance and integrity.

In 2016, CBP Enterprise Services (ES) was created to foster improved service delivery and increase collaboration among mission-support offices; providing essential resources and services to CBP as a whole. The offices that form ES support both frontline operators and non-frontline entities by providing a suite of products and services ranging from facilities management, information technology, and training, to congressional budget formulation and hiring.

Being responsible for multiple crucial, but often disparate roles, demands a responsive and flexible IT enterprise and workforce that enables frontline operators and mission support personnel to do their jobs efficiently and effectively.

CBP's Enterprise Services (ES) Office of Information and Technology (OIT) enables the timely exchange of data and communications for more than 60,000 employees, 185,000 trade users, thousands of external law enforcement trusted partners, and tens of millions of individual travelers.

The Assistant Commissioner (AC) of OIT serves as the CBP Chief Information Officer (CIO). The AC is supported by Infrastructure and Support Services (ISS) and Software Applications and Services (SAS), each of which are led by a Deputy Assistant Commissioner. This structure provides execution and oversight over the full scope of infrastructure responsibilities while encouraging a unified approach to enterprise solutions that serve the CBP mission and Trusted Partners. These two organizations are supported by Cybersecurity, Governance, and Technology organizations to ensure all OIT solutions are secure, standardized, compliant, efficient, and sustainable.

OIT must balance the daily challenges of delivering consistent access to secure data with the longer-term development of game-changing technologies that address CBP's needs in real time, while managing budget, risk, acquisition, and workforce considerations.



A TYPICAL DAY IN OIT

OIT'S WORK ENABLED CBP TO PROCESS/SUPPORT:



868,867
passengers and pedestrians

41 arrests of
wanted criminals
and



1,377 refusals of inadmissible
persons at U.S. ports of entry

63,843

CBP employees including



25,836
CBP



20,653

agents, and

700

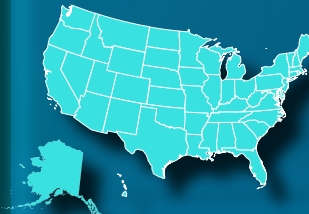
canine teams
deployed



91,605
truck, rail, and
sea containers



3,179
apprehensions
between U.S.
ports of entry



\$306
million in duties,
taxes, and other
fees



107,000

entries of merchandise
at U.S. air, land, and
seaports of entry



\$9.2
billion worth of
imported products
and over



185,000

Trade users

240 pests
discovered at U.S. ports of
entry and

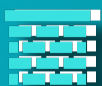


2,677
materials
discovered for
quarantine



328

ports of
entry within



20

field
offices and



129

Border Patrol
stations within



22

sectors

\$40 billion data
exchanges, **8** billion
queries, and
hundreds of thousands of
end point devices secured

226,589
incoming privately
owned vehicles



2,895
pounds of drugs
Seized



II. STRATEGIC ALIGNMENT

This CBP IT Strategy for Fiscal Years 2023-2027 describes OIT’s approach to support CBP’s mission to safeguard the American people, the national economy, and the United States’ air, land, and maritime borders. OIT is accountable for accelerating the incorporation of new technologies and innovations and then getting them to the frontline. Accomplishing these goals requires OIT to do its part in building a shared CBP culture, investing in the people who serve the country with passion, and positioning CBP for near and long-term success. Along the way, OIT must ensure that its services are well-integrated with the other functions in CBP’s Enterprise Services (Human Resources Management, Training and Development, Facilities and Asset Management, Programming, Accountability, and Acquisitions) to efficiently meet mission needs.

As part of DHS, CBP OIT must align its strategy to the Secretary’s mission and information technology priorities. OIT enables CBP to meet DHS’ goals of securing and managing American borders (through air, land, and sea) and safeguarding and expediting lawful trade and travel. A critical department priority is to address systemic and catastrophic cybersecurity risk through timely communications between national security entities and industry partners. OIT must do its part to enable the DHS IT sector to confront all potential threats.

Finally, this strategy is aligned to the President’s Management Agenda, National Security Strategy, and Federal CIO Policies and Priorities.

CBP IT Strategy progress is tracked in the CBP IT Executive Dashboard, where data visualizations make progress available to OIT stakeholders to enhance data-driven decision making.

Administration	
President’s Management Agenda	National Security Strategy, Federal CIO
Department of Homeland Security	
DHS Strategy & Mission Priorities	DHS IT Strategy & CIO Priorities
U.S. Customs and Border Protection	
MISSION - Protect the American people and facilitate trade and travel.	
TEAM - Build a sustainable, capable workforce that is adaptable and resilient in the face of dynamic challenges.	
FUTURE - Improve CBP capability to support operationally focused, threat-based, intelligence and data-driven execution.	
Enterprise Services	
PEOPLE - Build & develop an engaged mission-ready ES workforce	
TRUST - Foster a culture of reliability, transparency, & accountability	
RESULTS - Deliver at the “speed of operations”	
Office of Information and Technology	
Mission Infrastructure Mission Applications Trusted Partners Cybersecurity Enterprise IT Governance CIO Business Operations	

III. OPERATING ENVIRONMENT

OIT operates under strict requirements and constraints that demand meticulous planning for challenges, such as diverse mission needs, geographic dispersion of OIT's customers, federal and agency budget considerations, and technological needs to resiliently collect, store, and disseminate information.

OIT must deliver services to some of the most remote areas of the United States and abroad, with an ever-increasing need for mobile, operator-friendly tools that use data-rich services. These modern systems tax current infrastructure and demand sophisticated analytic capabilities. OIT also responds to high priority emerging operations such as international migration surges, hurricanes, and national security events such as the Super Bowl.

CBP's mission attracts committed adversaries who target IT systems with cyber-attacks. OIT must stay ahead of these exponentially increasing threats by deploying innovative and reliable tools that disrupt criminal activity and external attacks, while supplying relevant data to CBP employees and trusted partners. For that purpose, OIT has implemented resilient systems, services, and operations with built-in redundancies to prevent disruptions that could create security risks and impact the nation's economic supply chain. Meanwhile, OIT must relentlessly pursue cost efficiencies to compensate for funding reductions due to shifting federal priorities and the economic impacts of events such as the COVID-19 pandemic that resulted in diminished fee funding from travel reduction.

These operational, technological, and fiscal challenges place incredible demands on OIT's people. The workforce must respond to evolving mission needs and create technology solutions for an intense, ever-changing, global 24/7 environment. In a highly competitive market for federal IT talent, OIT must be a preferred place for diverse professionals to work and grow.



IV. VISION AND MISSION

OIT VISION

Getting the right information to the right people on any authorized device, anywhere, at any time.

CBP's IT vision is focused on deployment of the right information and technology to defend the U.S. and to facilitate a secure flow of international trade and travel, enabling an adaptable and resilient workforce, and supporting operationally focused, threat-based intelligence, and data-driven mission execution.



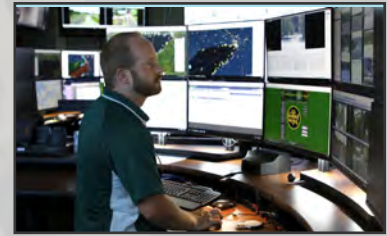
OIT MISSION

Deliver secure, reliable IT services and capabilities anywhere, anytime at the speed of CBP's 24/7 mission.

V. OIT VALUES - OIT VISION IN PRACTICE

OIT will achieve its vision by putting into practice the new **Values** we've established.

To develop and enhance solutions, OIT maintains a **Mission Focus** and continually advises customers on the state of emerging technology solutions that could improve their mission and business activities. OIT personnel are trusted partners of CBP's frontline and support personnel. They know the intrinsic, unspoken customer needs, are experts in technology solutions and the vendors that provide them, and are skilled in problem-solving techniques to overcome obstacles.



CBP OIT Values and Exemplary Behaviors

Utilize the exemplary behaviors to help incorporate our shared OIT values into your work and take time to recognize colleagues who live them out.

 MISSION FOCUS	 PEOPLE	 DIVERSITY	 COLLABORATION	 INNOVATION
<p><i>Act with purpose and unity to improve mission impact</i></p>	<p><i>Invest in our people and maintain integrity in pursuing our values</i></p>	<p><i>Respect and include a variety of people, cultures, and experiences to enhance products, services, and performance</i></p>	<p><i>Foster collaboration and openness among directorates and mission partners</i></p>	<p><i>Encourage innovative and resilient solutions for efficient and reliable delivery</i></p>
<p>DEMONSTRATING THESE VALUES IN YOUR DAILY WORK MIGHT LOOK LIKE:</p>				
<ul style="list-style-type: none"> Communicating the mission impact when explaining work accomplishments and/or risks Advocating for exposure or inclusion in mission partner-facing meetings Demonstrating an interest in learning about the mission impact Reaching out directly to a trusted partner to get clarifying instructions/information to better serve them Checking in with the business owner 9-12 months after implementation to confirm the solution met mission needs 	<ul style="list-style-type: none"> Recognizing the accomplishments of others Encouraging colleagues to pursue new training or learning opportunities (e.g., rotations) Proactively providing feedback to enable colleague growth and development Encouraging and enabling the well-being of others Outlining clear expectations for yourself (or your team); following up on progress and admitting when something is not accomplished Taking time to connect with your team on a personal level to build trust and relationships 	<ul style="list-style-type: none"> Practicing allyship by speaking up when you see or hear inappropriate behavior Organizing events to showcase the diversity of CBP employees Demonstrating curiosity and willingness to learn about the experiences of colleagues Consistently ensuring all voices are heard in meetings and giving those who have not contributed the chance to speak Soliciting a variety of perspectives, including those you may not always turn to, when making a decision or solving a problem 	<ul style="list-style-type: none"> Building relationships across OIT directorates to improve mission partner service Proactively sharing work updates on progress to increase transparency Demonstrating interest in the work of others by asking intentional questions Connecting the dots between concepts, ideas, or technology to encourage a united OIT Making an effort to partner with and share information and materials across teams and directorates 	<ul style="list-style-type: none"> Identifying new ideas to streamline/improve operations Exploring new opportunities to integrate new technology solutions to improve mission partner experience Translating industry trends to OIT's environment and recommending improvements Adjusting and staying flexible when there is new information or changing circumstances Taking initiative to solve a problem without being asked Encouraging your team to consider how to improve efficiency with the available time and resources

OIT systems and tools are always available and reliable, providing the information and insight customers need to do their jobs all the time, everywhere. OIT systems are as reliable as every other piece of equipment officers, agents, and other CBP employees use to do their jobs.

To achieve this capability, OIT invests in its **people** to improve their skills, work environment, and the overall capacity to perform their work. OIT personnel know what skills and outcomes are expected from them. OIT empowers them to develop their capabilities and holds them accountable for performance. As a desirable place to start and continue a career, OIT celebrates **diversity** required to attract highly

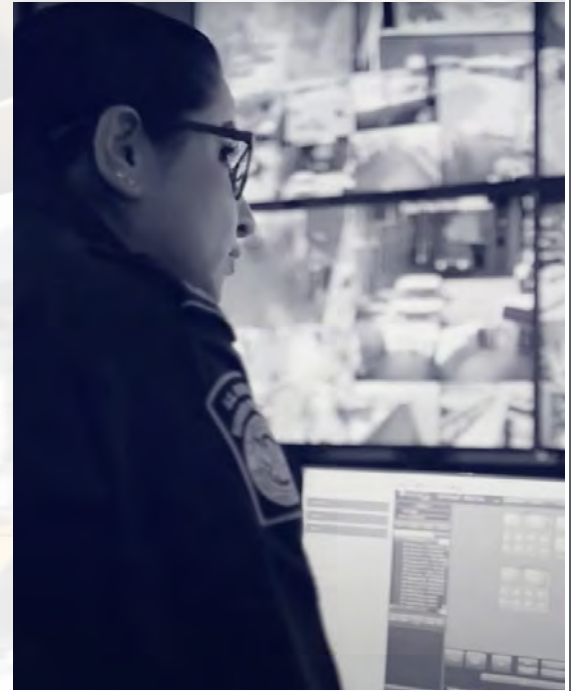
skilled and motivated people from all backgrounds who continuously learn from industry leaders, partners, and each other.

As a collaborative and transparent organization, OIT personnel are empowered and expected to speak up. They take appropriate risks, work across organizational structures, and demonstrate the initiative and innovation needed to stay ahead of customers' needs. OIT works as one team in **collaboration** with trusted partners to pursue **innovation** as OIT provides the resources, insight, and executive guidance necessary to support customers, solve problems, and enhance the collective work experience of CBP personnel.

Strategic Goals and Objectives

The CBP IT Strategy outlines six Strategic Goals and underlying Strategic Objectives that represent the changes—to OIT culture, people, trusted partner collaboration, and solution delivery—that OIT has committed to implement to achieve OIT’s vision.

These goals and objectives are further enabled by prioritized initiatives staffed with project teams. While the vision describes the OIT aspirations and the goals define the OIT focus, these initiatives lay out the fundamental capabilities that OIT must achieve. OIT goals create a framework to build these capabilities through improved processes, empowered and capable people, and new technology solutions that deliver customer value and enable mission-critical support.



OIT STRATEGIC GOALS

Goal 1: Mission Infrastructure

Continuously provide innovative near-real time infrastructure capabilities to ensure a secure, reliable, and scalable IT Infrastructure at the speed of CBP’s mission through collaboration with application teams and our trusted partners to accelerate and optimize delivery



Goal 2: Mission Applications

Build mission-aligned applications that are more reliable and scalable, leveraging a domain-driven design to access centralized shared services based on user requirements



STRATEGIC OBJECTIVES

Objective 1.1: Consolidated Enterprise Network Establish a modern integrated network with edge-to-edge security

Objective 1.2: Core Enterprise Cloud Computing Provide a scalable and cost-effective cloud services and transparent operations for data-driven decisions and rapid response

Objective 1.3: IT Operations Ensure reliability and availability of applications, systems, data, and information that drive mission operations and decision making

Objective 2.1: Digital Experience Provide access to IT resources in a timely manner at any location on any authorized device through user-friendly interfaces

Objective 2.2: Enterprise Data Management Institute data practices, methods, and technologies to ensure data is holistic, trustable, accessible, and interoperable

Objective 2.3: Application Development Facilitate iterative development of scalable and secure capabilities provisioned in a resilient environment

Objective 2.4: Scalability Enhance scalability of enterprise application capabilities through collaboration with infrastructure teams to provide the right information to the right people on any authorized device

Goal 3: Trusted Partners

Administer a Trusted Partner Program that responds to the technology needs of our partners to anticipate, influence, and deliver on expectations by understanding needs sooner, finding collaborative solutions, and improving customer experience



Objective 3.1: Integration and Transparency Increase IT initiative integration and transparency within CBP offices and the enterprise

Objective 3.2: Interagency Relationships Establish interagency relationships with other government law enforcement agencies

Objective 3.3: Industry and International Partners Identify and establish relationships with potential industry and international partners

Goal 4: Cybersecurity

Close the gap between increasingly sophisticated and persistent threat actors and CBP's adoption of the right technology, people, and processes in order to improve security of CBP's technology assets and increase protection of the mission by implementing proactive, risk-based cybersecurity practices that create a strong and resilient security posture for CBP systems, networks, and data



Objective 4.1: Cyber Hygiene Defend mission operations by improving cyber hygiene as an effective and cost-efficient way for CBP to keep its networks safe by striving for central and comprehensive visibility into its IT infrastructure and assets

Objective 4.2: Threat Detection and Response Improve threat detection and response capabilities by implementing endpoint detection and response (EDR) technology, deception technology, and user behavior analytics; instituting proactive cyber threat hunt activities; and leveraging its existing cybersecurity toolset to enhance threat detections and reduce attack surface

Objective 4.3: Cyber Protection Shift CBP cyber protection from primarily perimeter-facing into a Zero Trust Architecture (ZTA) while maintaining availability and minimizing temporal delays in cloud migration effort (CME)

Objective 4.4: Cybersecurity Governance, Risk Management, and Compliance Involve all of CBP in cybersecurity governance, risk management, and compliance to maintain a strong cybersecurity posture

Goals 5: Enterprise IT Governance

Improve IT governance capabilities, resources and tools to maximize enterprise-wide efficiencies through disciplined performance

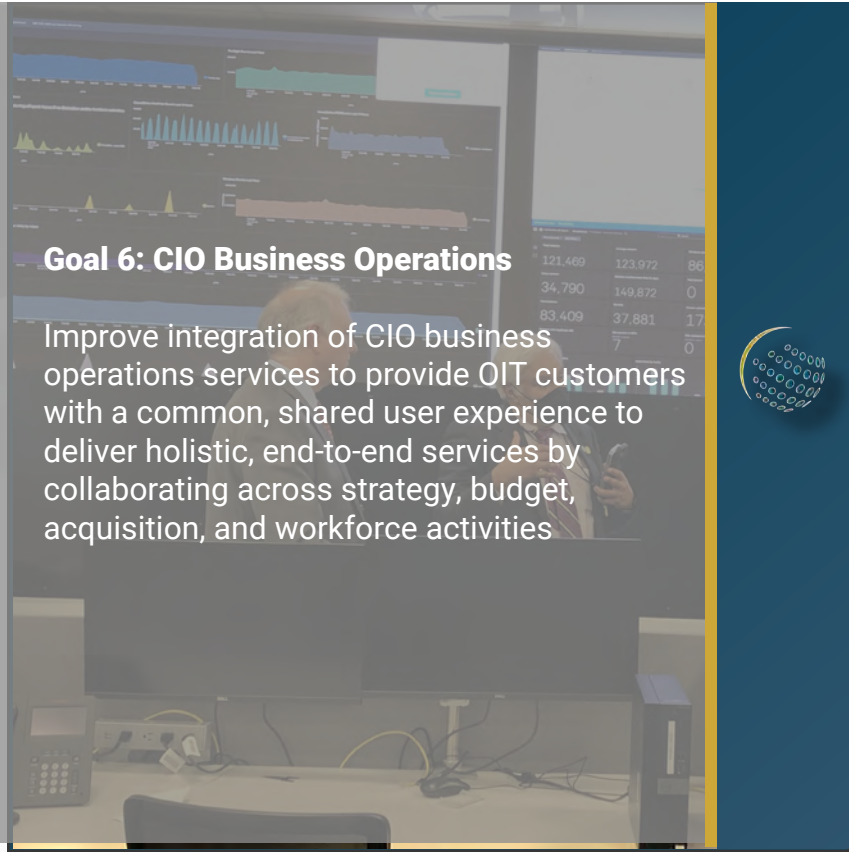


Objective 5.1: Governing Policies / Processes Provide a decision-making framework to achieve consistency and standardization in governing new and existing technologies and associated business processes through increased integration and visibility of policies and directives for decision-makers

Objective 5.2: Governance Boards Integrate enterprise-wide IT governance processes to improve cross-function decision-making to support mission interoperability and decision-sharing across the enterprise

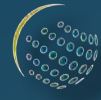
Objective 5.3: Compliance Improve alignment of federal, department, and agency IT-related regulations, policies, and directives as well as OIT policies and standards to better support program teams with compliance

Objective 5.4: Communications, Education and Coordination Ensure all CBP employees understand their roles in governance to engage in consistent and efficient approaches to compliance across the enterprise



Goal 6: CIO Business Operations

Improve integration of CIO business operations services to provide OIT customers with a common, shared user experience to deliver holistic, end-to-end services by collaborating across strategy, budget, acquisition, and workforce activities



Objective 6.1: Strategy Management

Mature the brokerage of enterprise IT business operations data and information to support evidence-based decision-making by increasing and improving business intelligence capabilities

Objective 6.2: Cost and Budget Transparency

Instill further rigor and discipline in financial and asset management to get to an informed, balanced budget and asset management strategy early in the fiscal year

Objective 6.3: Procurement / Acquisition Support

Implement a disciplined approach to requirements definition to improve OIT contract strategies through internal planning, collaboration, and engaging with the procurement division early in the acquisition process

Objective 6.4: OIT Workforce Experience

Enhance employee growth and development opportunities that improve the OIT workforce experience to help employees realize individual career objectives

Objective 6.5: Workforce Management

Strive for a diverse, qualified, and empowered IT workforce at 98% on board to achieve the CBP mission





DHS CIO FY 2022 Priorities

Compliance

Diversity, Equity, and Inclusion (DE&I)

Customer Experience (CX)

Enterprise Infrastructure Solutions (EIS)

Cybersecurity

Technology Modernization Fund (TMF)

... CBP: A DAY IN THE LIFE (FY 2022) ...

- Processed 868,867 passengers and pedestrians
- 226,589 incoming privately owned vehicles
- \$9.2 billion worth of imported products
- 107,000 entries of merchandise at our air, land, and sea ports of entry
- \$306 million in duties, taxes, and other fees
- 2,895 pounds of drugs seized

National Key Significant Events

Uniting for Ukraine (U4U)

Operation Allies Welcome (OAW)

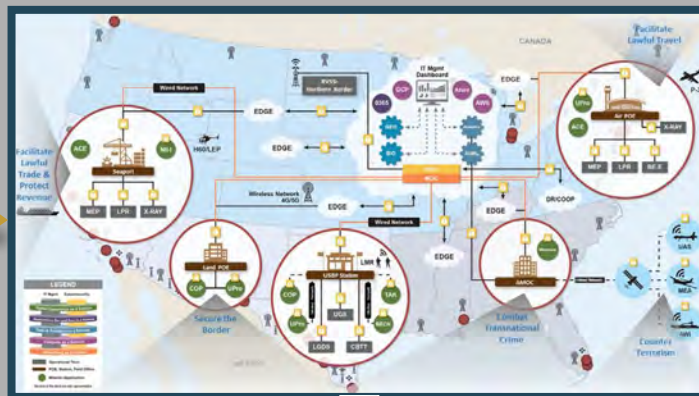
Super Bowl LVI

Southwest Border Migrant Surge

COVID-19

CBP OIT Support

CBP's IT landscape is expansive and provides 24/7 mission support across 1,744 locations nationally. OIT meets enterprise mission needs using capabilities and tools developed to modernize infrastructure, improve cybersecurity, and expand enterprise applications.



INTRODUCTION



Enterprise Architecture assists in optimizing the interdependencies among CBP's mission and business operations, and the underlying IT and IRM that support them.

OIT'S STRATEGIC FOCUS AREAS

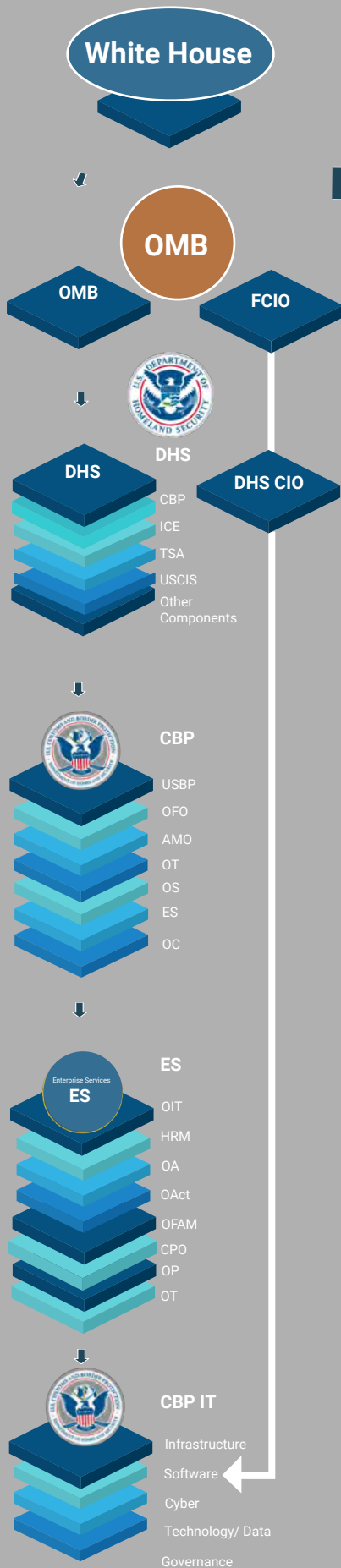


The expansion and enhancement of dashboards continued in FY 2022 and was a priority project that further streamlined access to information, enhanced transparency, and improved delivery.

FUTURE VISION

OIT will strive to deliver enterprise services and applications at the speed of mission. OIT will use the tools it has developed to keep modernizing, enhancing cybersecurity, increasing network connectivity, and support ongoing innovations to keep pace with evolving mission needs.

AGENCY STRATEGY



IMPLEMENTATION

MISSION



CBP Mission

Protect the American people, safeguard our borders, and enhance the nation's economic prosperity.

OIT Mission

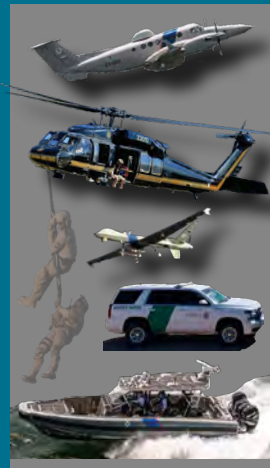
Deliver secure, reliable IT services and capabilities anywhere, anytime at speed of CBP's 24/7 mission.

OUTCOMES

- FASTER
- BETTER
- MORE AFFORDABLE
- MORE SECURE

TECHNOLOGY ENVIRONMENT

OPERATIONAL TECHNOLOGY



INFORMATION TECHNOLOGY



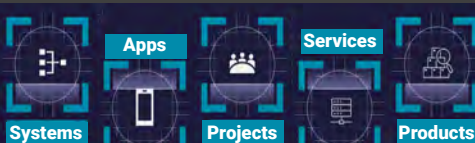
STRATEGIC APPROACH

- Strategic Transformation
- Tactical Excellence
- Innovation

OIT'S STRATEGIC FOCUS AREAS



TECHNOLOGY PORTFOLIO



MEASUREMENT



SUPPORTING STRATEGIES

MISSION INFRASTRUCTURE

- Consolidated Enterprise Network
- Core Enterprise Cloud Computing
- IT Operations

MISSION APPLICATIONS

- Digital Experience
- Enterprise Data Management
- Application Development
- Scalability

TRUSTED PARTNERS

- Integration & Transparency
- Interagency Relationships
- Industry & International Partners

MISSION CYBERSECURITY

- Cyber Hygiene
- Threat Detection & Response
- Cyber Protection
- Cybersecurity Governance, Risk Management, and Compliance

ENTERPRISE IT GOVERNANCE

- Governing Policies / Processes
- Governance Boards
- Compliance
- Communications, Education & Coordination
- Enterprise Architecture & Data Governance
- TRM+TRA+Data Governance

CIO BUSINESS OPERATIONS

- Strategy Management
- Cost and Budget Transparency
- Procurement / Acquisition Support
- OIT Workforce Experience
- Workforce Management
- Portfolio Management

CUSTOMER EXPERIENCE (CX)

Assist lead business authority develop enterprise customer service operating model to further mature CBP's customer experience capabilities



MISSION INFRASTRUCTURE



Always Safe. Always Secure. Always-on, Mission Support!

Continuously provide innovative, near-real time infrastructure capabilities to ensure a secure, reliable, and scalable IT Infrastructure at the speed of CBP's mission through collaboration with application teams and our Trusted Partners to accelerate and optimize delivery



[READ MORE](#)

Infrastructure and Support Services Strategy

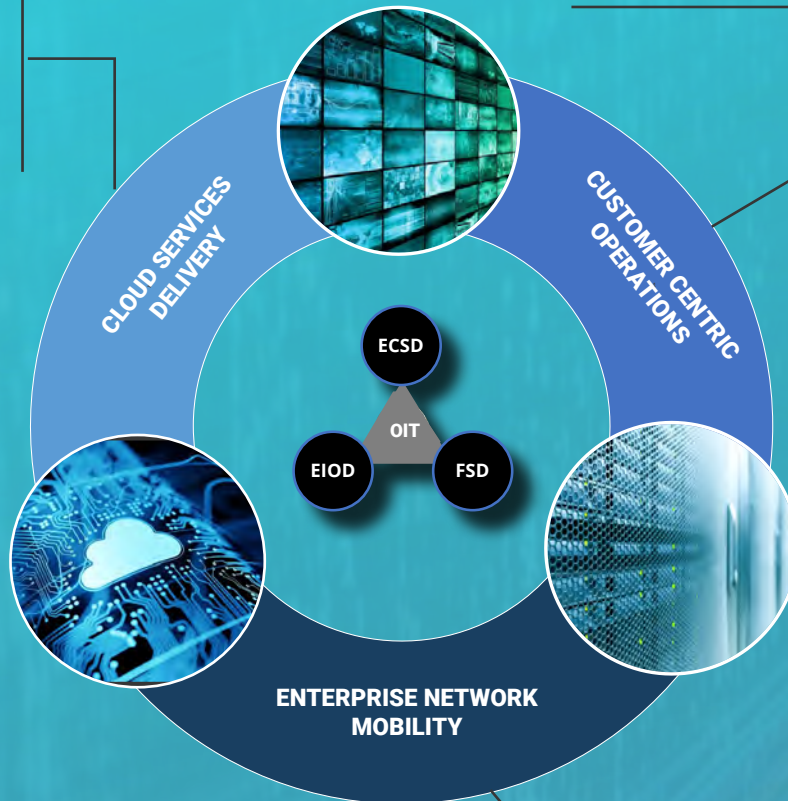
Deliver secure, reliable IT services and capabilities anywhere, anytime at the speed of CBP's 24/7 mission

CLOUD SERVICES DELIVERY

Provide access, tools, capabilities and services for needs today and tomorrow through automation, auto-provisioning, and other new methods to optimize customer experiences

CUSTOMER CENTRIC OPERATIONS

Continuously improve all aspects of CBP mission infrastructure support and maintenance to best serve IT and our customers 24/7



ENTERPRISE NETWORK MOBILITY

ENTERPRISE NETWORK MOBILITY

Build and enhance CBP network capabilities for fast and secure access to a wide range of services, capabilities and applications needed to support the mission

MISSION INFRASTRUCTURE

Always Safe. Always Secure. Always-on, Mission Support!

GOAL 1: Mission Infrastructure

Continuously provide innovative near-real time infrastructure capabilities to ensure a secure, reliable, and scalable IT Infrastructure at the speed of CBP's mission through collaboration with application teams and our Trusted Partners to accelerate and optimize delivery

SEVEN SERVICES OF IT AT CBP



Enterprise Data Management

Data Practices, methods, and technologies to ensure data is holistic, trustable, accessible, and interoperable



Network

Establishment of a modern integrated network and edge-to-edge security



Digital Experience

Access to IT resources in a timely manner at any location on any devices through user friendly interfaces



Cybersecurity

Safeguarded information assets through secure development, simplified identity controls, mitigation of malicious activity



Application Development

Iterative development of scalable and secure capabilities provisioned in a resilient environment



IT Management and Delivery

Transparency of all IT operations, management, and costs for data-driven decision



Compute

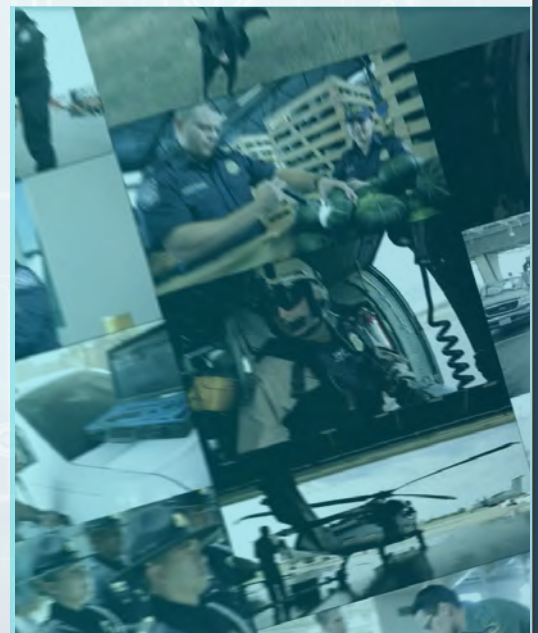
Provision of scalable and cost-effective cloud services and transparent operations for data-driven decision and rapid response

ORGANIZING OUR PRIORITIES

Objective 1.1: Consolidated Enterprise Network

Establish a modern integrated network with edge-to-edge security

- Converge data and voice networks to lower expenditures, reduce complexity, increase availability, and improve security by decreasing on-premises, obsolete voice systems
- Expand network availability to mobile locations to enable mission operation flexibility by increasing the number of locations with effective wireless access
- Centralized network: Work with Office of Finance (OF) to consolidate network resources and funding in OIT in-order-to treat networking as a utility, ensure tech refresh, and optimize bandwidth



Objective 1.2: Core Enterprise Cloud Computing

Provision of scalable and cost-effective cloud services and transparent operations for data-driven decisions and rapid response

- Establish CBP/OIT multi-cloud strategy/ solution that provides flexible and scalable infrastructure while controlling costs and securing data
- Eliminate obsolete mainframe as a service to avoid annual recurring costs
- Establish Enterprise Cloud Services Team to facilitate and optimize cloud deployments



Success Story: SAP FY22 Cloud Migration



- In continual collaboration with OF, OIT completed the cloud migration of CBP Financial Solutions System (SAP) from National Data Center (NDC) to Amazon Web Services (AWS) and the migration of the SAP Business Warehouse to a High Performance ANalytic Appliance (HANA) in-memory database

- The SAP Program had a very high risk opened for the past 11 years (opened February 2011) for the aging hardware used by the SAP Business Warehouse Accelerator (BWA). The solution to the risk was to migrate from an Oracle database to a HANA in-memory database for the SAP Business Warehouse

- **Key Benefits:** The AWS environment is a more modern, sustainable, resilient, and scalable cloud platform that provides the baseline for the growth and expanded capabilities for the SAP Program:



Eliminate the need to purchase physical devices, allowing faster modernization to a newer technology; Provide the Financial System with a Disaster Recovery strategy; Ability to provide high availability for priority systems in the future; New back-up plan developed using cloud tools, no longer dependent on Netbackup Appliance on-premises



- Migrated all of SAP Landscapes to the Cloud – 5 non-prod and 1 production (SBX, DEV, QA, Q2, TRN, and PROD) – Lift & Shift

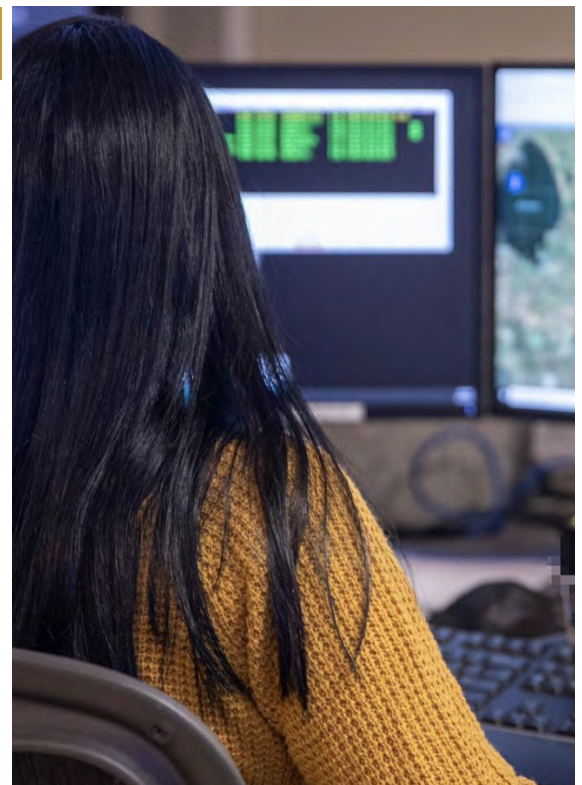


- The migration consisted of migrating 131 Vessel Management SYSTEM (VMS) (60 databases, 71 app servers) from NDC to the AWS cloud, re-establishing 80+ connections (for each environment: non-production and production) and validating 160+ interfaces. Approximately 60TB of data was migrated to the cloud

Objective 1.3: IT Operations

Ensure reliability and availability of applications, systems, data, and information that drive mission operations and decision-making

- Obtain enterprise funding for end-user equipment, field network infrastructure, and circuit modernization sufficient to meet mission requirements and emerging priorities while conforming with industry standards & security compliance
- Transform end user services to enable more productive tools for the remote worker
- Determine and maintain optimal tech to CBP employee ratio and establish dedicated VIP/executive support
- Assess and, where possible, transition U.S. Border Patrol (USBP) Program Management Office Directorate (PMOD) and Office of Field Operations (OFO) technologies from Contract Logistics Support (CLS) to organic OIT Support



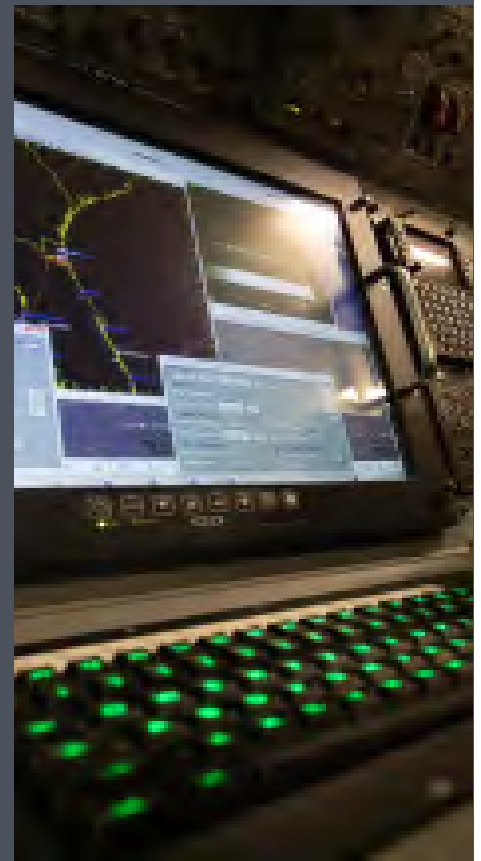


MISSION APPLICATIONS

#2 GOAL

INNOVATIVE AND RESILIENT SOLUTIONS *at the Speed of Mission*

Build mission-aligned applications that are more reliable and scalable, leveraging a domain-driven design to access centralized shared services based on user requirements



READ MORE

Software Applications & Services Strategy

Deliver secure, reliable IT services and capabilities anywhere, anytime at the speed of CBP's 24/7/ mission

APPLICATION DEVELOPMENT

Facilitate iterative development of scalable and secure capabilities provisioned in a resilient environment.



DIGITAL EXPERIENCE

Provide access to IT Resources in a timely manner at any location on any authorized device through user-friendly interfaces.



Application Development

Digital Experience

Scalability

Enterprise Data Management

BEMSD CSPD
TASPD PSPD

SCALABILITY

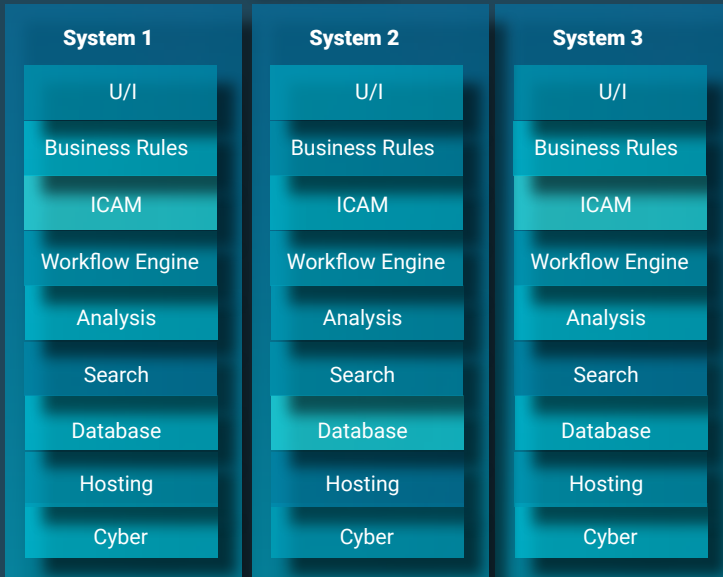
Enhance scalability of enterprise application capabilities through collaboration with infrastructure teams to provide the right information to the right people on any authorized device.



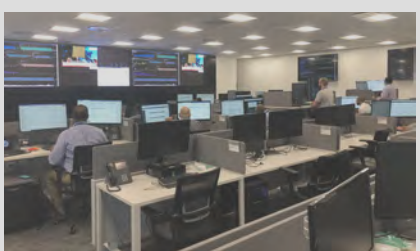
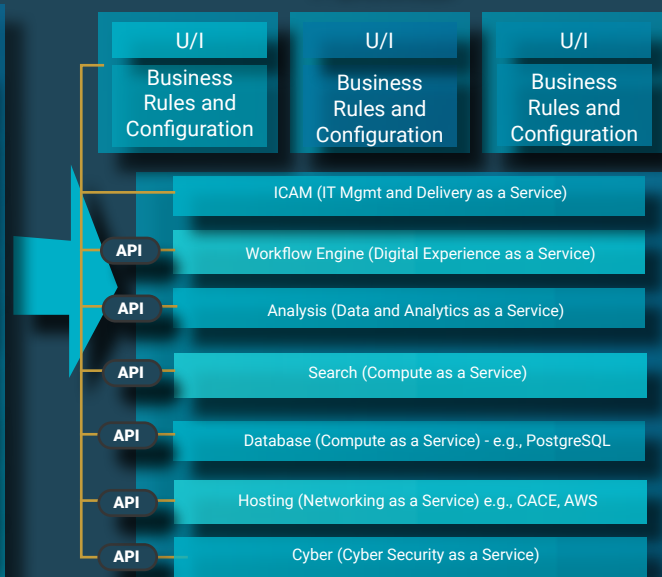
ENTERPRISE DATA MANAGEMENT

Institute data practices, methods, and technologies to ensure data is holistic, trustable, accessible, and interoperable.

CURRENT



PLANNED



“Innovation and technology infrastructure needs must be constantly developed at the speed of mission, and our Trusted Partnership with OIT meets this requirement.”

– Donald R. Stakes, Executive Director
Mission Support Directorate
Office of Field Operations (OFO)

MISSION APPLICATIONS

INNOVATIVE AND RESILIENT SOLUTIONS at the Speed of CBP's 24/7 Mission

GOAL 2: Mission Applications

Build mission-aligned applications that are more reliable and scalable, leveraging a domain-driven design to access centralized shared services based on user requirements

Today, applications are built to support particular CBP programs and data resides in program-specific systems. These systems are not easily scalable and capabilities are duplicated across programs. Officers, agents, and analysts often struggle with data discovery, access, and sharing.

In the future, OIT will help build mission-aligned applications that are more reliable and scalable leveraging a domain-driven design to access centralized shared services based on user requirements. In other words, the mission provides the rules and configuration while leveraging OIT-provisioned IT services. More specialized technologies will be managed by the mission and supported by OIT.

Example: As numbers of undocumented noncitizens continued to increase throughout 2021 and 2022, CBP identified a priority need to standardize how the organization performs case processing and custody management. A joint team was formed to create a single application, Unified Processing (UPRO), that provides operational flexibility and a readily trained surge force that can immediately respond to changing tactical situations in either domain. The solution consolidates the functions of two existing applications, Unified Secondary and e3, and leverages enterprise IT services, aligns to federal IT mandates, and provides capability at best cost.



Objective 2.1: Digital Experience

Provide access to IT resources in a timely manner at any location on any authorized device through user-friendly interfaces

- Deliver applications that seamlessly span the suite of CBP authorized devices and that integrate with the relevant core mission data sources
- Provide a cloud-based, unified toolset that is accessible across multiple channels to support on-site, hybrid, and remote work
- Improve self-service and automation capabilities to support increasingly complex Trusted Partner engagements
- Ensure consistent customer data and programmatically aligned processes to facilitate customer journeys, with multiple touchpoints across departments and technologies



Success Story:

Uniting for Ukraine (U4U)

• OIT collaborated with the Office of Field Operations (OFO) to develop and deploy the Advanced Traveler Information System (ATIS), which vets applicants to provide advance authorization to travel to the U.S., allows evacuees to seek parole, and integrates with the CBPOne scheduling application to allow applicants arriving at land POE to schedule traveler appointments

• DHS allowed U.S. sponsors to submit an I-134 Declaration of Financial support to U.S. Citizenship and Immigration Services (USCIS). This allows Ukrainian citizens and immediate family members to apply for advance authorization to travel to the U.S., where they can seek parole for a period of up to two years

• OIT created a dashboard for CBP and DHS containing information about Ukrainian nationals arriving to the U.S. through the USCIS I-134 sponsorship process as well as daily arrivals from Mexico. OIT also established a data share with USCIS to report post arrival information

• OIT, in close collaboration with OFO and USCIS, established an interface to transmit beneficiaries' information from USCIS to CBP, which allows CBP to conduct vetting for advance travel authorization, provide the approval/denial notification to USCIS, and notify beneficiaries through MyUSCIS





- OIT implemented a U4U hotlist within the Unified Passenger (UPAX) application that is integrated with the National Vetting Center (NVC) and ATS applications to automate traveler vetting against law enforcement databases, allow for manual vetting by the National Targeting Center (NTC), and provide NTC with an indicator of classified vetting results

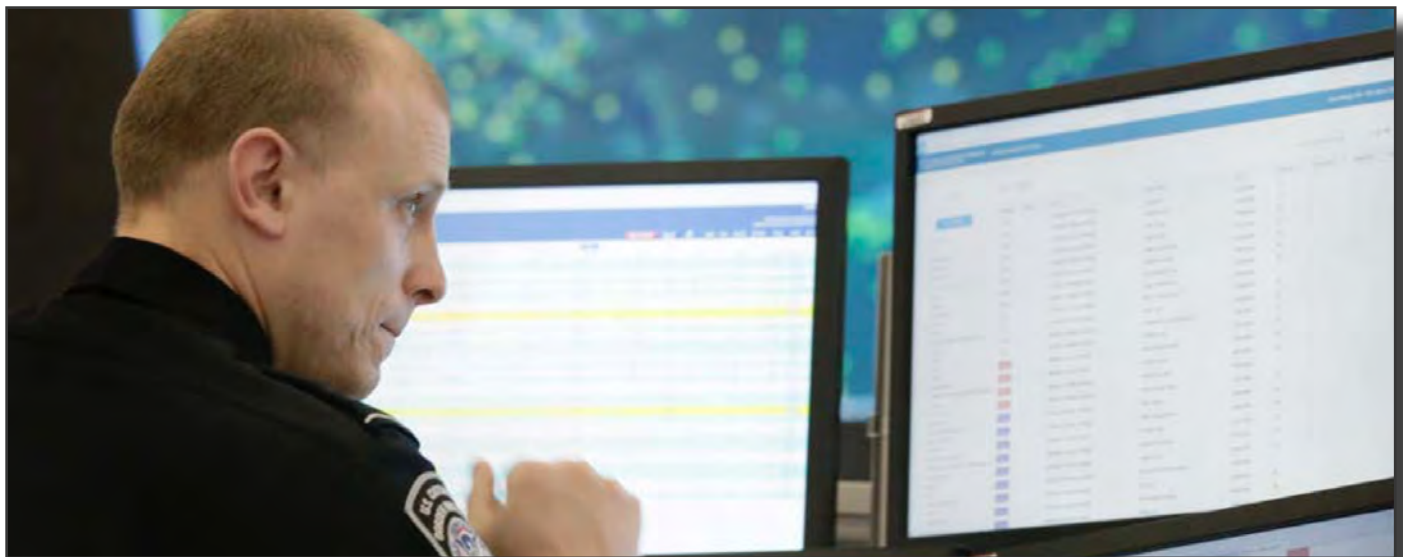
Objective 2.2: Enterprise Data Management

Institute data practices, methods, and technologies to ensure data is holistic, trustable, accessible, and interoperable

- Transform data management processes to address evolving data requirements, interoperability, quality, and reporting
- Leverage appropriate emerging technologies to provide scalable, flexible, and responsive data solutions to meet mission needs
- Promote information sharing and related enterprise-wide capabilities to provide for discovery, access, trust, usability, and analysis of data
- Develop and empower a skilled workforce to use data responsibly and ethically to make informed decisions



MISSION APPLICATIONS



CBP Data Strategy

Goal Four: Sustainable Data Culture

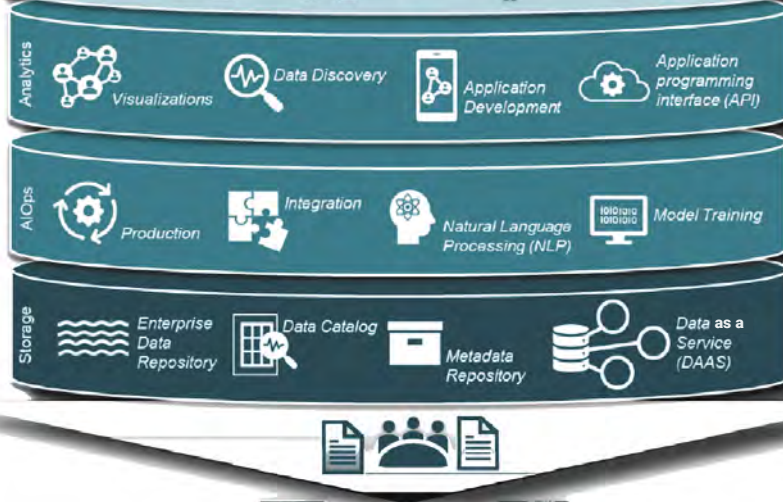
Develop and empower a skilled workforce to make informed decisions



Goal Three: Enterprise Information Sharing Capability
Promote information sharing and related enterprise-wide capabilities to provide for discovery, access, trust, and usability of data

Goal Two: Data Technology Optimization
Leverage emerging and appropriate technologies to provide scalable, flexible, and responsive data solutions to meet mission needs

Goal One: Enterprise Data Management
Transform data management processes to address evolving data requirements and interoperability



Holistic
Data is comprehensive and understandable

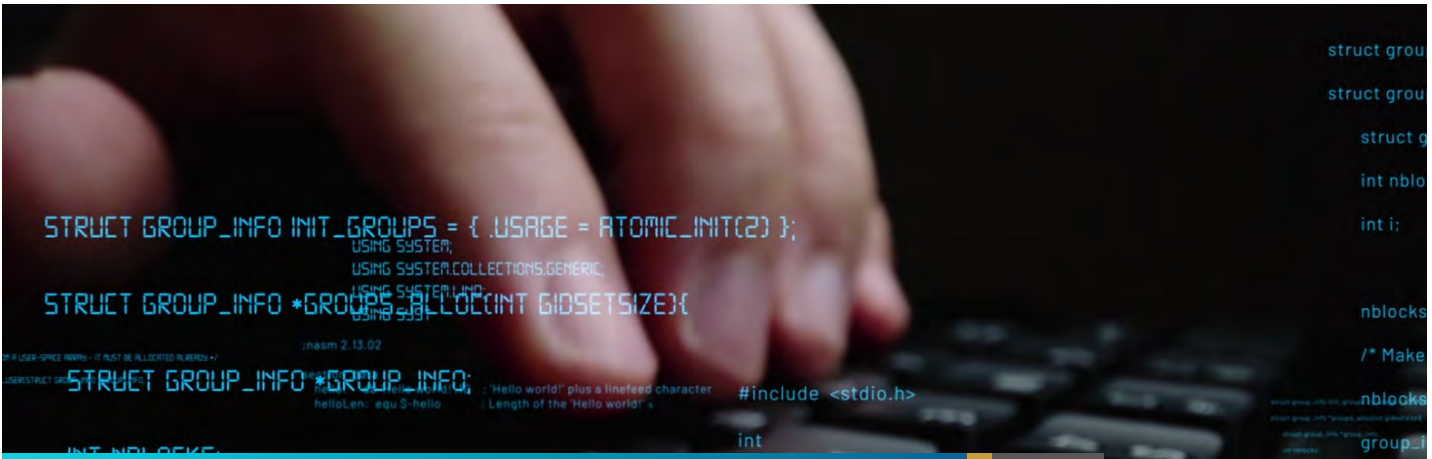
Trustable
Accurate, secure and reliable data throughout the enterprise lifecycle

Accessible
Dynamic access, scalability, cost effectiveness and greater discoverability of data

Interoperable
Data is easily retrieved, used, shared, and processed across various CBP systems and applications



MISSION APPLICATIONS



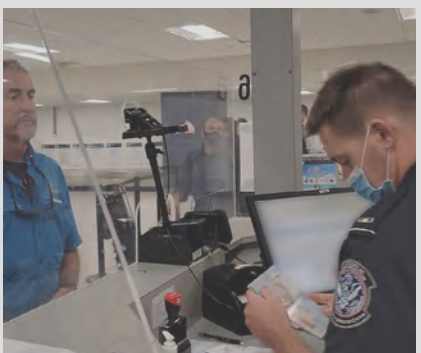
“In a Digital Age where data connectivity, provenance, access, and security are paramount, USBP recognizes that Information Technology is a crucial enabler to effective border security. CBP’s IT Strategy 2023-2027 positions CBP OIT to keep pace with USBP’s growing IT demands, dynamic mission, and rapid technology advancement taking place in the private sector.”

– Christ Pietrzak,
Acting Deputy Executive Director
Program Management Office
U.S. Border Patrol (USBP)

Objective 2.3: Application Development

Facilitate iterative development of scalable and secure capabilities provisioned in a resilient environment

- Drive a cloud native-first approach to cross-platform development that includes the browser, creating new options for write once, run everywhere
- Increase capabilities that enable people to work effectively from anywhere, on any authorized device
- Reorient recruiting practices for jobs beyond OIT's local markets and be prepared to face strong competition for the best and brightest



Success Story:

Unified Immigration Portal (UIP) Enhancements

- Provided users with access to critical subject-level information on-the-go or in the field by allowing users to view contract tracing reports, subject level details, Time in Custody (TIC) arrest history, and medical logs on their mobile devices

- Deployed the Credible Fear Referrals Dashboard to provide a more complete view of credible fear processing from U.S. Immigration and Customs Enforcement (ICE) to USCIS custody which includes subject-level details, fear claimed dates, referral dates, and referral decision dates as credible fear subjects are referred from ICE to USCIS and are accepted or rejected for credible fear interviews

- Deployed the U.S. ICE Detentions Dashboard to provide users with historic details of subjects detained in ICE facilities and trends of subject book-in and book-out numbers, improving coordination and increase efficiencies during handoffs between U.S. CBP and ICE

- Enabled DHS to process subjects for vaccinations more easily by integrating the uVax application with UIP's Biographic Service which automates biographic details for subjects in custody from UIP's service, significantly reducing the need for manual processes

Objective 2.4: Scalability

Enhance scalability of enterprise application capabilities through collaboration with infrastructure teams to provide the right information to the right people on any authorized device



Streamline governance processes, tools, and skills for modern architectures, to mitigate risks of applications failing to meet expectations and deliver business value



Develop distributed architectures with simpler components but increased integration capabilities to meet rapidly changing business needs



Create environments conducive to skill building and differentiating OIT as an employer of choice



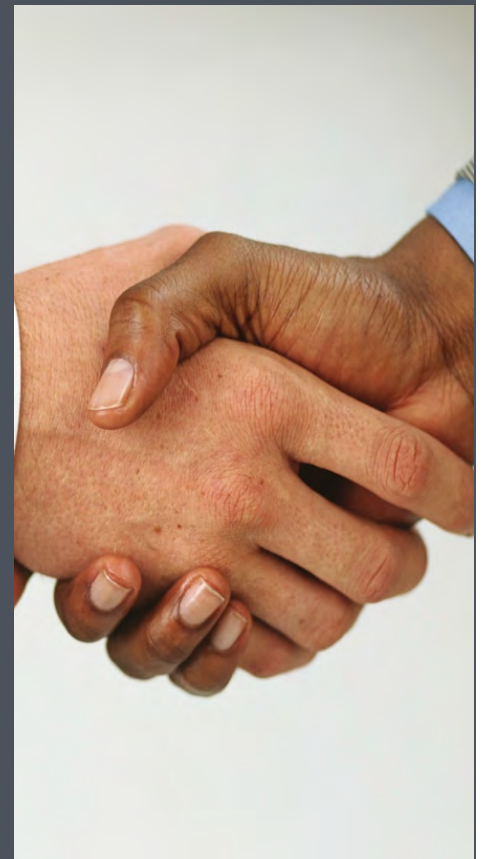


TRUSTED PARTNERS

#3 GOAL

Building Solutions Together

Administer a Trusted Partner Program that responds to the technology needs of our partners to anticipate, influence, and deliver on expectations by understanding needs sooner, finding collaborative solutions, and improving customer experience



[READ MORE](#)



TRUSTED PARTNERS

Building Solutions Together

GOAL 3: Trusted Partners

Administer a Trusted Partner (TP) Program that responds to the technology needs of our partners to anticipate, influence, and deliver on expectations by understanding needs sooner, finding collaborative solutions, and improving customer experience

OIT's success depends on teaming with trusted partners and customers. Understanding and respecting what each group brings, partnering with one another to co-create and deliver solutions, and setting and managing expectations enables us to deliver exceptional services to meet their mission needs



Innovation

The Trusted Partnership Initiative (TPI)

Structured Framework

The Trusted Partnership Initiative (TPI):

strategically and tactically delivers IT to operate at the speed of mission, seamlessly, digitally, reliably, and securely

Innovation:

OIT partnered with the CBP Innovation Team (INVNT) to deliver leading-edge Silicon Valley and Intelligence Community solutions (e.g., AI/ML, RPA) with better alignment and 3x faster program delivery to mission needs

Structured Framework:

OIT delivered an agile, scalable program framework of strategic transformation built upon tactical excellence. A baseline program portfolio is established for each stakeholder



Objective 3.1: Integration & Transparency

Increase IT initiative integration and transparency within CBP Offices and the enterprise

- Implement standard operating procedure (SOP) for running the Trusted Partner (TP) Program, including audit trails and related procedures which track the implementation of guidance and the completion of action items from partner meetings
- Business intelligence insights and optimized resource allocation
- Standardization of dashboards
- OIT brand integrity measured by partner, customer, and stakeholder satisfaction
- Collaborative solutions and improved IT services
- Improved and increased support for emerging priorities



Success Story:

Operations Allies Refuge/
Operation Allies Welcome (OAR/OAW)

• OIT helped control the logistics of thousands of people fleeing Afghanistan while managing risks posed by extremist activity. OIT coordinated with federal agencies, international partners, and commercial airlines to conduct thorough security screenings of non-U.S. citizens and permanent residents, and to validate US citizens evacuated. In the early days of the evacuation, OIT provided critical support to Department of State (DoS) to help identify American citizens and Lawful Permanent Residents who still needed to be evacuated from Afghanistan. OIT mobilized immediately and effectively to play a critical part in the largest airlift in U.S. history, ensuring CBP was able to process over 86,000 evacuees and help deliver travelers to their destination/safe haven

• In support of Operation Allies Welcome (OAW), OIT developed several new solutions to process evacuees from Afghanistan. These included biometric and biographic collection, targeting and vetting, data stream consolidation and sharing with partner agencies, and subsequent validation of vetting results using photo comparison services. This led to advancements in automated processes to merge vetting results into one repository for verification prior to boarding flights to the U.S.



• In creating this central repository to consolidate vetting results, OIT leveraged photos from biometric enrollments to build a photo gallery; using ATS Mobile Query, CBP personnel stationed at OCONUS locations verified vetting results using facial matching technology, providing a highly reliable method for identifying the vetting results for all biometrically enrolled individuals and allowing boarding of flights to the U.S.



• OIT created a dashboard for CBP and DHS containing information about Ukrainian nationals arriving to the U.S. through the USCIS I-134 sponsorship process as well as daily arrivals from Mexico. OIT also established a data share with USCIS to report post arrival information



• OIT created a modular, OAW dashboard to provide statistics on passengers arriving to the U.S. as part of the Afghanistan evacuation efforts. Statistics on the dashboard provided DHS and CBP management and officers in the field close to real time updates on Primary and Secondary processing of Afghanistan evacuees, unaccompanied minors, and U.S. Citizens



• OIT continues to provide 24/7 operational coverage, making numerous improvements to data sharing applications, creating interoperability between DoD, CBP, DoS, USCIS, and the Transportation Security Administration (TSA), and maintaining the OAW dashboard, which provides daily status for DHS/CBP OFO to track number of flights, travelers processed, enrollment, and vetting

Objective 3.2: Interagency Relationships

Establish interagency relationships with other government law enforcement agencies

- Implement SOP for running the trusted partner (TPI) initiative, including audit trails and related procedures which track the implementation of guidance and the completion of Action Items from partner meetings
- Cross-agency collaboration on IT solutions, information sharing, and resources
- OIT brand integrity measured by partner, customer, and stakeholder satisfaction
- Collaborative solutions and improved IT services
- Improved and increased support for emerging priorities

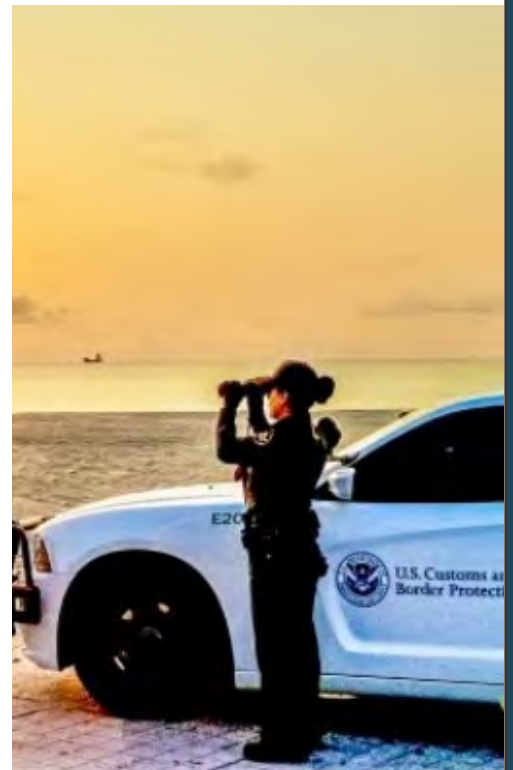


The TPI strategically and tactically delivers IT to operate at the speed of mission - seamlessly, digitally, reliably, and securely.



“Through their Trusted Partnership meetings, OIT emphasizes clear communications and productive collaboration to ensure our organization stays informed. Issues are raised and resolved more efficiently due to OIT’s enthusiasm for sharing with their CBP partners.”

– Trevor Blow
Executive Director, Mission Support
Air and Marine Operations (AMO)



Objective 3.3: Industry and International Partners

Identify and establish relationships with potential industry and international partners

- Implement SOP for running the TPI, including audit trails and related procedures which track the implementation of guidance and the completion of Action Items from partner meetings
- Improved leveraging of technology best practices and standards across CBP/OIT
- OIT brand integrity measured by partner, customer, and stakeholder satisfaction
- Collaborative solutions and improved IT services
- Improved and increased support for emerging priorities

OIT's commitment to excellence, professionalism, and "can-do" team approach with all stakeholders has built relationships and "street credentials" with agents/officers on the frontlines with a "force multiplier effect" in a tough law enforcement culture.

Success Story:

International Trusted Partner Accomplishments

- Coordinated with 98 countries to improve national security and travel for 60 million incoming international passengers to the U.S.
- Established a technology roadmap with "five-eye" countries in the Border 5/Migration 5 (B5M5) CIO Tech Forum for border security technology and Touchless Borders of the Future

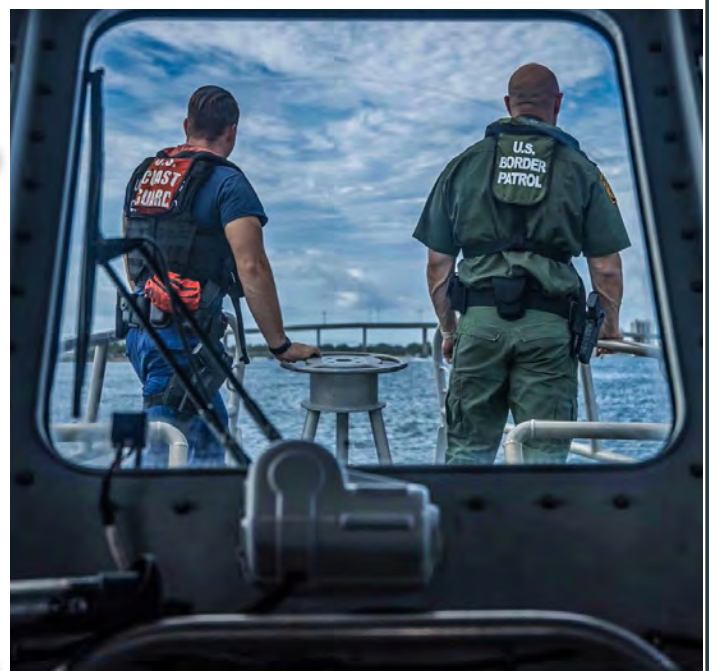


As a Trusted Partner, OIT focuses on how it can best support a valuable relationship at a global scale.

Success Story:

Industry Trusted Partner Accomplishments

- Supported over 162,000 users in the trade community with \$4 trillion in imports/exports, largest collections (\$96 billion)
- 1st DHS program to be awarded the General Services Administration (GSA), Technology Modernization Fund (TMF)



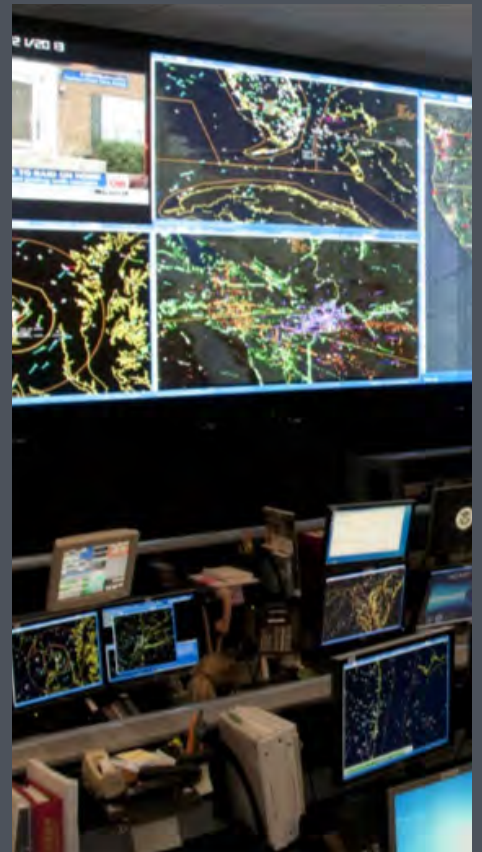


CYBERSECURITY

#4 GOAL

Protecting the IT Enterprise

Close the gap between increasingly sophisticated and persistent threat actors and CBP's adoption of the right technology, people, and processes in order to improve security of CBP's technology assets and increase protection of the mission by implementing proactive, risk-based cybersecurity practices that create a strong and resilient security posture for CBP systems, networks, and data



[READ MORE](#)

CYBERSECURITY

Protecting the IT Enterprise

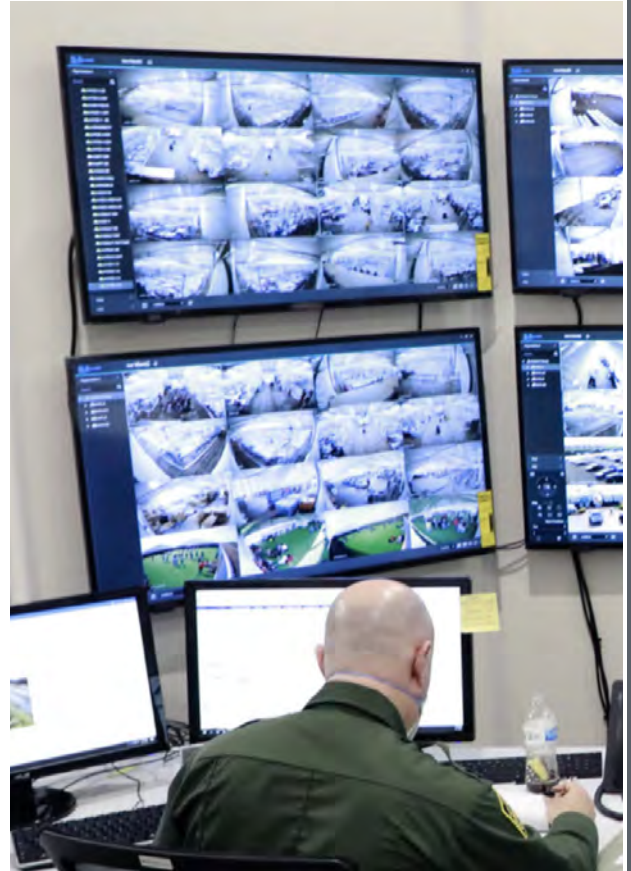
GOAL 4: Cybersecurity

Close the gap between increasingly sophisticated and persistent threat actors and CBP's adoption of the right technology, people, and processes in order to improve security of CBP's technology assets and increase protection of the mission by implementing proactive, risk-based cybersecurity practices that create a strong and resilient security posture for CBP systems, networks, and data

CBP's strategic cybersecurity goal will close the gap between increasingly sophisticated and persistent threat actors and CBP's adoption of the right technology, people, and processes. Shifting and competing priorities make it difficult for federal agencies to maintain state-of-the-art capabilities, but without effective cybersecurity measures, CBP's entire mission is at risk. It is vital that every CBP employee, stakeholder, and partner fully recognize and appreciate the direct connection between sound cybersecurity practices and the national security of the United States.

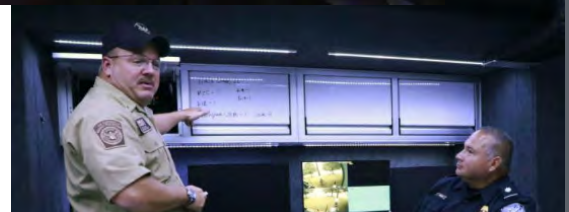
"OIT is one of our primary partners in safeguarding both national and economic security. Their innovative solutions have allowed us to explore and develop cutting edge technologies that let us keep pace with an ever-evolving trade environment and to protect American consumers and American business from unsafe products and unfair trade practices. We simply could not perform the important work we do without OIT's insight and expertise. We look forward to our continued partnership as the Office of Trade implements new strategies to tackle key enforcement priorities like forced labor, supply chain resiliency, and sustainability."

– AnnMarie Highsmith
Executive Assistant Commissioner
Office of Trade (OT)



Objective 4.1: Cyber Hygiene

Defend mission operations by Improving cyber hygiene as an effective and cost-efficient way for CBP to keep its networks safe by striving for central and comprehensive visibility into its IT infrastructure and assets



Cyber Threats to CBP Systems

- Protect CBP data, systems, and networks from unauthorized access
- Improved visibility of CBP information technology and data to identify and remediate vulnerabilities
- Routinely perform penetration testing on CBP operational systems to identify vulnerabilities requiring remediation
- Protected continuity of mission operations through improved network and data resiliency

Cyber hygiene refers to basic practices that users can take to secure their systems, such as regularly updating systems antivirus protections and software. Promoting and implementing cyber hygiene principles is an effective and cost-efficient way for CBP to keep its networks safe.

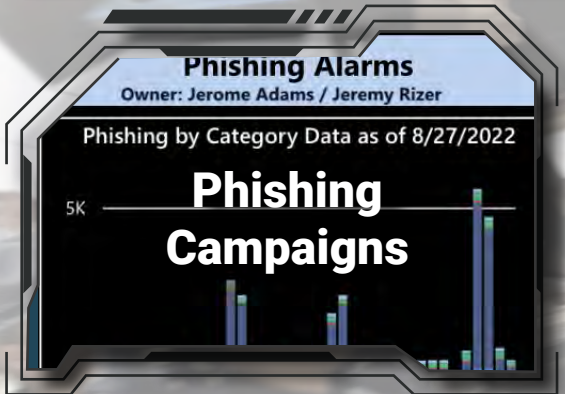
In keeping with federal priorities on cyber hygiene, CBP will work to transition its security capabilities away from an ad hoc, reactive approach towards a proactive and multi-layered defense against cybersecurity threats. To achieve this, CBP must continue to strive for central and comprehensive visibility into its IT infrastructure and assets. This central management of assets will enable effective control of access to CBP networks and data, protecting mission-sensitive data from leakage and preventing unauthorized access.

These threats will continue to evolve and be used in attempts to penetrate CBP systems in order to monitor, destroy, steal, or hold hostage critical information.

Objective 4.2: Threat Detection & Response

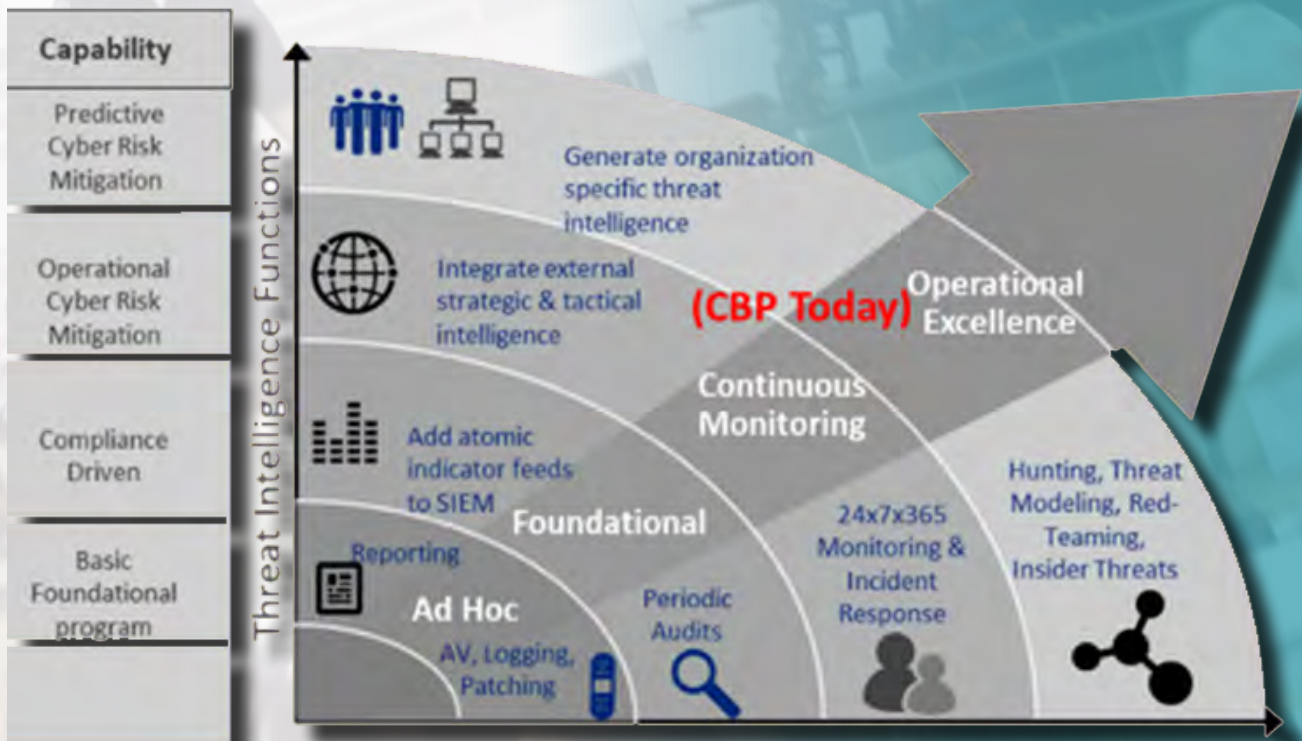
Improve threat detection and response capabilities by implementing EDR technology, deception technology, and user behavior analytics; instituting proactive cyber threat hunt activities; and leveraging its existing cybersecurity toolset to enhance threat detections and reduce attack surface

- Expanded threat detection and security monitoring capabilities
- Improved Cyber Threat Intelligence Capabilities and Information Sharing to Enhance Detection and Insight into Cyber Threats



While prevention of cyber incidents through cyber hygiene is key to a hardened security posture, CBP recognizes that it is impossible to fully prevent all cyber-attacks. Therefore, a crucial part of CBP's security defenses is to maintain continuous insight into network operations and respond to cyber incidents through its Security Operations Center (SOC). CBP will strive to strategically improve its cyber threat detection capabilities by implementing endpoint detection and response (EDR) technology, deception technology and user behavior analytics; instituting proactive cyber threat hunt activities; and leveraging its existing cybersecurity toolset to enhance threat detections and reduce attack surface.

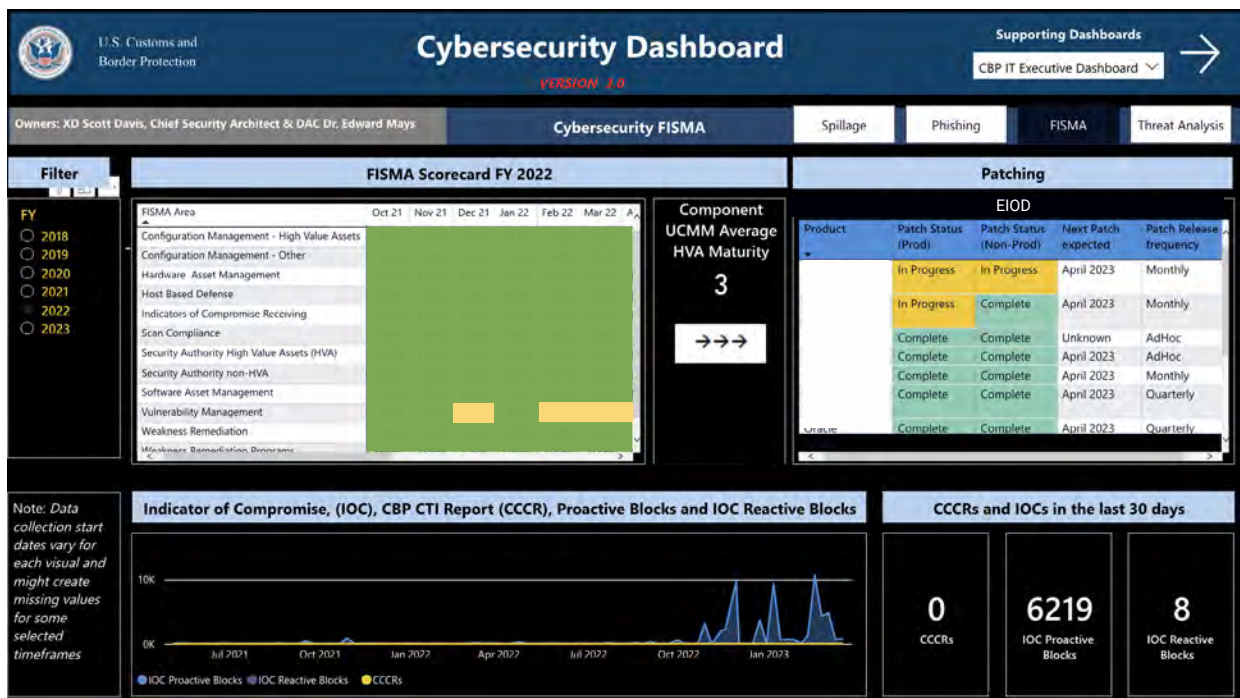
Intelligence gathering and information sharing are critical to holistically monitoring and understanding the scope of the cyber threat landscape. CBP will continue to build out its threat intelligence platform to automate indicator of compromise (IOC) collection and queries, while fostering information sharing with OIT's intelligence community (IC), Department of Defense (DoD), and public-private sector partners. In addition, CBP will continue to expand its monitoring of network administrator and privileged user account activity for abnormal or malicious behavior. Privileged account compromise is a primary target of cyber adversaries and insider threats.



Objective 4.3: Cyber Protection

Shift CBP cyber protection from primarily perimeter-facing into a Zero Trust architecture while maintaining availability and minimizing temporal delays in cloud migration effort (CME)

- Develop and implement a more robust cybersecurity model



CBP Zero Trust Architecture (ZTA) strategy for cyber security provides the opportunity to create a more robust and resilient security, simplify security management, improve end-user experience, and enable modern IT practices. It is a cybersecurity strategy and framework that embeds security throughout the architecture to prevent malicious personas from accessing the organization's most critical assets. It provides zones for visibility and security mechanisms positioned throughout the architecture to secure, manage, and monitor every device, user, application, and network transaction occurring at the perimeter and/or within a network enclave. The CBP ZT strategy directly supports the President's Executive Order on Improving the Nation's Cybersecurity – Modernizing Federal Government Cybersecurity.

Success Story:
Trusted internet connection (TIC) 3.0 with Zero Trust architecture (ZTA)

- Implemented TIC 3.0 based on a ZTA migrated 700 trade partners and government agencies

- This brings OIT customers closer to CBP applications, improves resiliency by eliminating dependency on DHS OneNet, improves intrusion detection/protection, and blocks over 10,000 bad actors

Objective 4.4: Cybersecurity Governance, Risk Management, and Compliance

Involve all of CBP in cybersecurity governance, risk management, and compliance to maintain a strong cybersecurity posture

- Lead the implementation of best-in-class cybersecurity policies and practices
- Consistently assess the security and privacy risks of CBP information and systems against compliance standards
- Develop and maintain a workforce to support evolving cybersecurity threats
- Improve the security posture of CBP by promoting cybersecurity awareness for all system users

All 60,000+ CBP employees play a critical role in leading, implementing, and maintaining effective cybersecurity, regardless of whether they are in the field or in an office. Engaging and educating all employees through role-based training is critical to maintaining a strong cybersecurity posture.

Enterprise-level security governance is critical for effective cybersecurity risk management, and CBP will continue to refine and enforce security policy, while fostering a culture of security awareness across the organization. Additionally, recruiting, developing, and retaining a cyber workforce that is equipped to work with new technologies and counter emerging threats is vital to protecting CBP's mission.



CBP IT STRATEGY 2023-2027



CBP'S Recent Cybersecurity Achievements

(as of Q4 FY2021) By the numbers



• Scan and protect against over **2M Indicators** of Concern. Average of **13 vulnerability** scans of **130K assets** monthly



• **3.8k potential** phishing emails reported via Phish Alarm button in last **30 days**. This is over **95% of all email reported** as potential phishing attempt



• **28 Cyber Threat** Intel Reports created and distributed to CBP and Federal partners



• Over **40 million** blocks on the proxies preventing unauthorized connections



• Granted Authority to Operate to 43 systems and added 10 to Ongoing Authorization

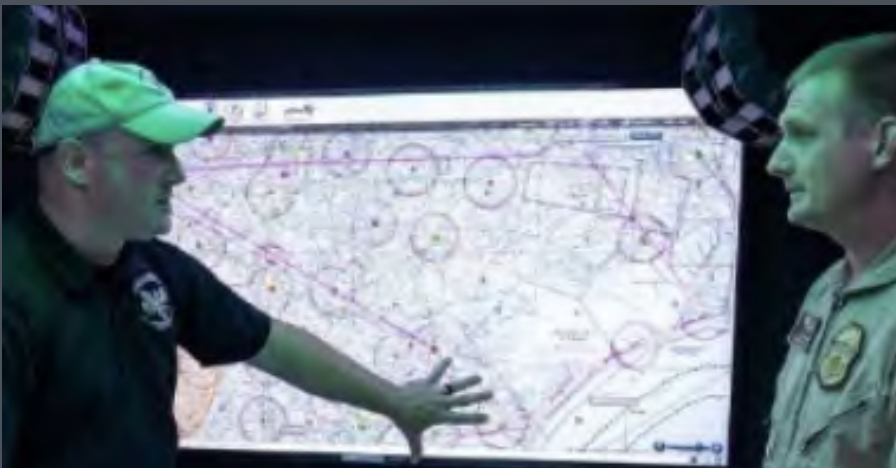


ENTERPRISE IT GOVERNANCE

#5 GOAL

STRUCTURE. DISCIPLINE. EXCELLENCE: *Getting IT Right*

Improve IT governance capabilities, resources, and tools to boost enterprise-wide efficiencies through disciplined performance



[READ MORE](#)

ENTERPRISE IT GOVERNANCE

STRUCTURE. DISCIPLINE. EXCELLENCE: *Getting IT Right*

GOAL 5: Enterprise IT Governance

Improve IT governance capabilities, resources, and tools to maximize enterprise-wide efficiencies through disciplined performance

OIT will establish the necessary governance policies, processes, boards, alignment, and communication mechanisms to increase standardization, compliance, and efficiencies and empower OIT's entire workforce to make data-driven decisions at the appropriate level.

MGD Mission Statement - *OIT's Management and Governance Directorate (MGD) will enhance IT management and governance for services and integration capabilities, resources, and tools that strengthens efficiency and effectiveness across the Enterprise. MGD is committed to providing both internal and external customers with consistent, highest quality user experience using disciplined performance standards and a commitment to excellence.*

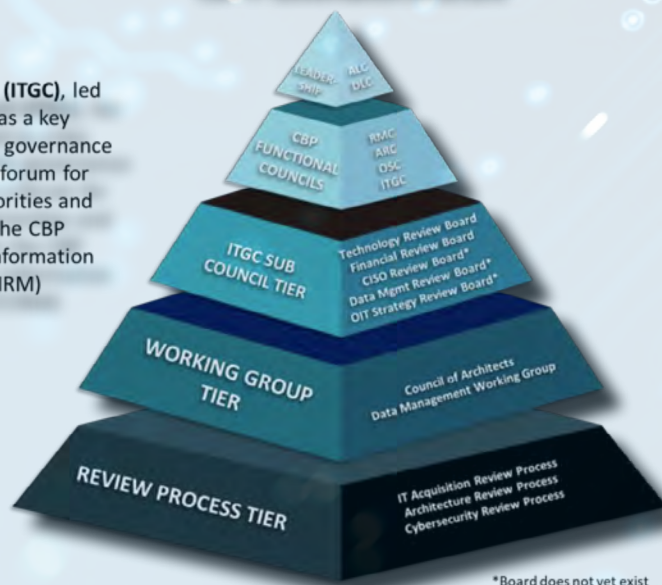
MGD Vision Statement – *OIT's MGD enables Mission Partners to achieve their priorities through holistic alignment of OIT's capabilities and business operations. MGD will provide structured business processes and policies, oversee capabilities to drive adaptable innovation, and improve delivery timeliness, quality and efficiency throughout OIT's lifecycle and service to Mission Partners.*

MGD Motto – *Consider IT Done.*

Objective 5.1: Governing Policies/Processes

CBP IT Governance Structure

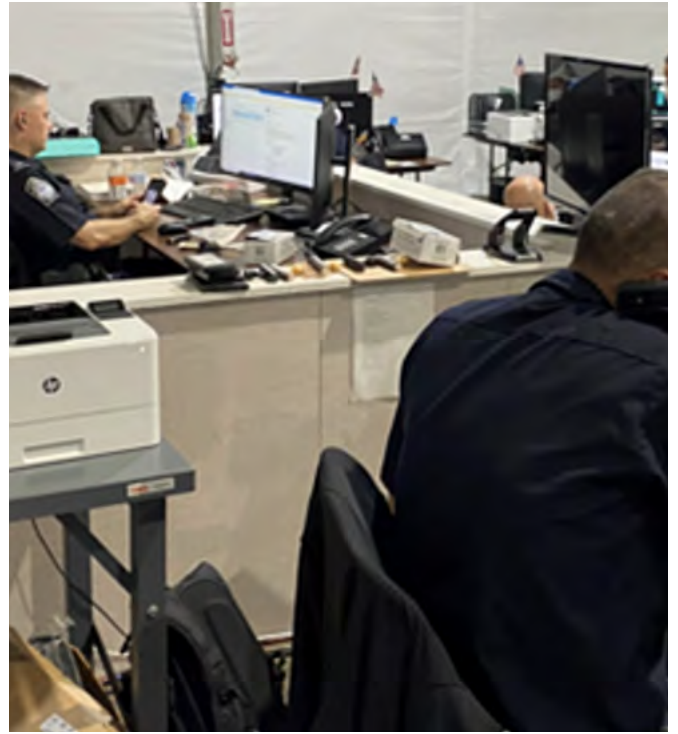
The IT Governance Council (ITGC), led by OIT's CIO, is established as a key element of CBP's corporate governance structure, designed to be a forum for leaders from CBP to set priorities and to provide governance for the CBP Information Technology / Information Resource Management (IT/IRM) enterprise.



The ITGC works as a focused body of empowered decision-makers responsible for implementing and operationalizing decisions and strategic direction provided by the DLC.

Provide a decision-making framework to achieve consistency and standardization in governing new and existing technologies and associated business processes through increased integration and visibility of policies and directives for decision-makers

- Active participation of stakeholders and partners
- Drive efficiencies through economies of scale (e.g., less tech spend; less duplication of tools/apps, etc.)
- Develop and publish a framework that is available to everyone and provides guidance from an integration perspective
- Increase in policy development to deliver better and more integrated policies and focus on efficiencies across the enterprise



Objective 5.2: Governance Boards

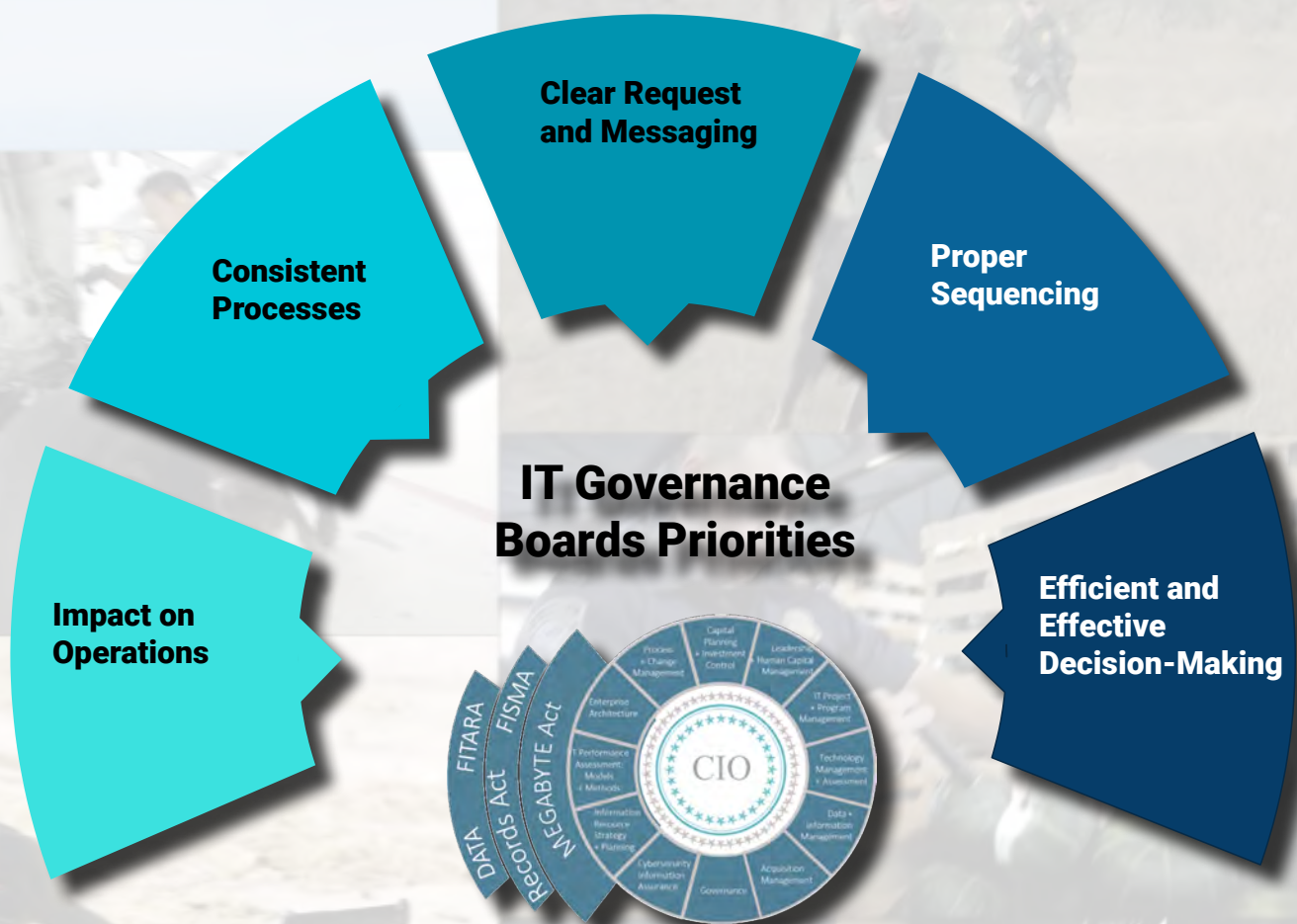
Integrate enterprise-wide IT governance processes to improve cross-function decision-making to support mission interoperability and decision-sharing across the enterprise

- Remove organizational stovepipes
- Establish end-to-end processes
- Cross-function requirements that begin with end mission/customer result in mind
- Share decisions across CBP governance boards



CBP's IT governance boards provide leadership direction and enable strategic IT decision-making in support of mission success across the enterprise. IT governance boards follow the agency's governance guiding principles as adopted by the Deputies Leadership Council (DLC). IT governance boards will prioritize the following:

IT Governance Boards Priorities



Impact on Operations: Briefings will focus on the operational impact of decisions on this topic, including the impact of inaction.



Clear Request and Messaging: Each briefing or agenda item will state a clear decision request or articulate the value of the information provided in advance of the meeting.



Efficient and Effective Decision-Making: IT governance councils facilitate cross-component dialogue, collaboration, and resolution of CBP-wide issues and challenges, and promote effective and efficient processes and support structures with overarching transparency, responsiveness, and accountability.



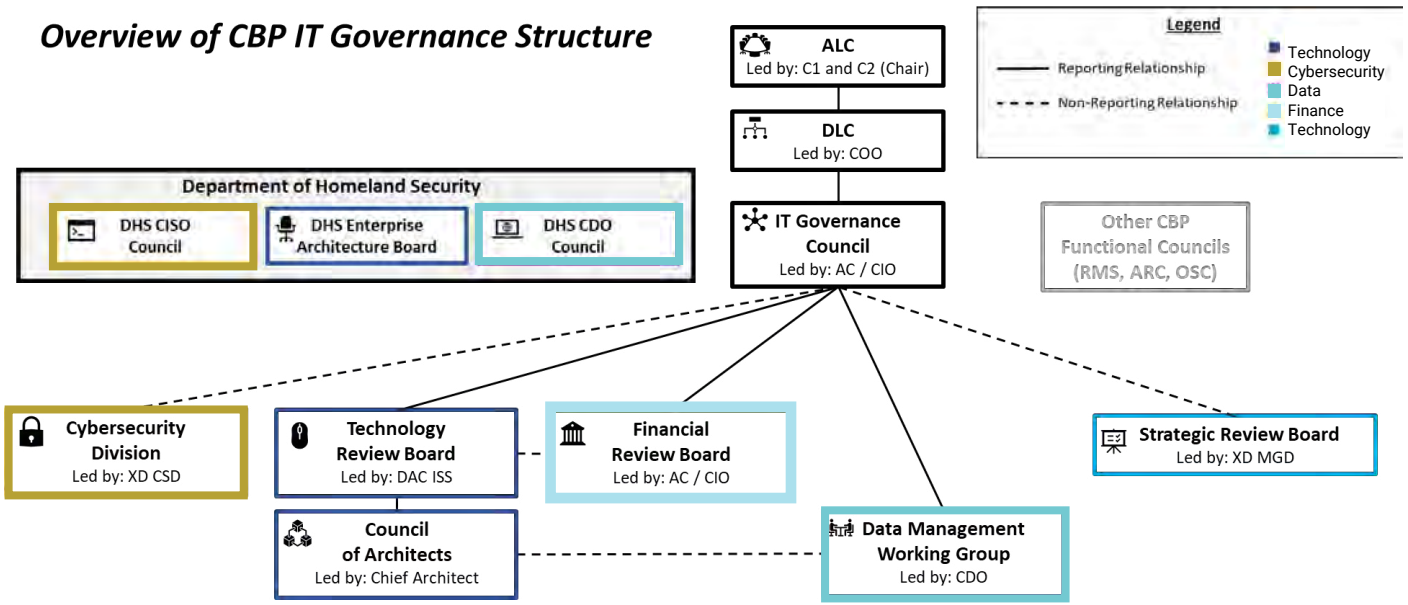
Consistent Processes: There shall be repeatable processes leading up to a governance meeting and following each meeting's conclusion to ensure all stakeholders are prepared for discussion.



Proper Sequencing: When possible, topics will be coordinated across the governance councils to allow for subordinate councils to review and make recommendations first before sending higher-level decisions up the governance hierarchy.

The ITGC will be a key governing body that helps to align CBP OIT stakeholders with internal and external stakeholders. Led by CBP's CIO, the ITGC is designed to be a forum for leaders from CBP to set priorities and to provide governance for the CBP Information Technology/Information Resource Management (IT/IRM) enterprise. For insight into IT Governance integration and operation, review the governance structure below:

Overview of CBP IT Governance Structure



Success Story:

CBP IT Governance Council (ITGC)

- Established the CBP ITGC to oversee CBP's entire enterprise Information Technology/Information Resource Management (IT/IRM) Portfolio of 73 investments, 179 Systems, 245 Projects, and 26 High Value Assets

- The ITGC meets monthly with Trusted Partners to discuss enterprise-wide technology governance as well as a bi-monthly deep dive sessions with each of the Trusted Partners to focus on their respective areas of responsibility with regards to IT governance

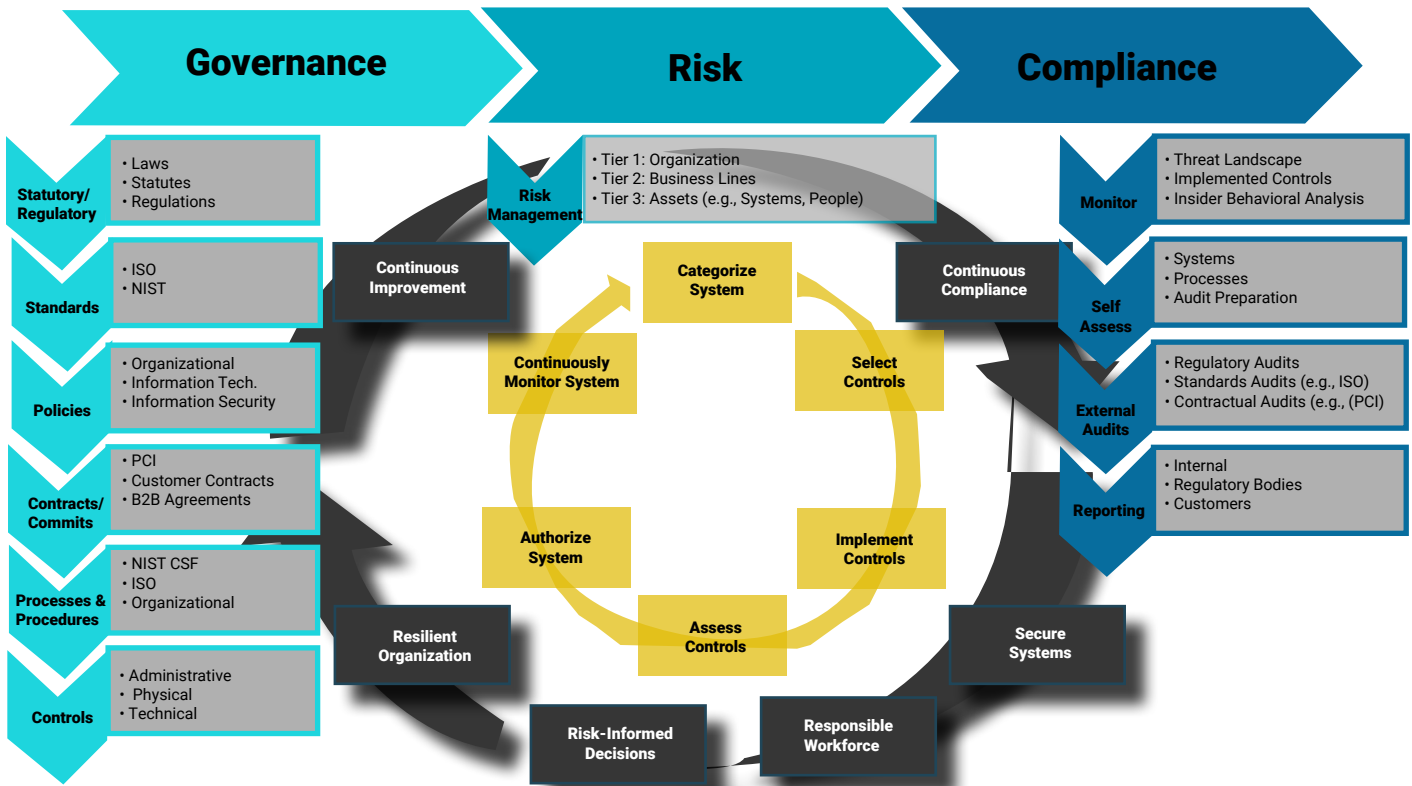
Through the implementation of three new review boards, OIT will have representation at the CBP/DHS level of governance in cybersecurity, strategy, and data management.



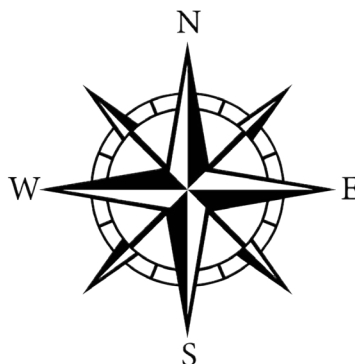
Objective 5.3: Compliance

Improve alignment of federal, department, and agency IT-related regulations, policies, and directives as well as OIT policies and standards to better support program teams with compliance

- Compliance requirements – definition and baseline
- Reduction in IT risk
- Policy mappings and tools
- Compliance mechanisms that support governance



OIT will push forward with implementing the best practice overarching governance structure above:



The IT Governance framework is in progress to align our IT strategy with our business strategy. OIT will articulate integral connectivity between ongoing OIT Governance, Risk, and Compliance workflows and support any gaps along the way. The IT governance framework embeds risk assessments into decision-making processes while better adhering to rules and regulations. This best practice will address the needs of the internal and external stakeholders and customers. Governance works best for all components of business and stakeholders when the necessary integration and collaborations are defined and supported. The IT Governance framework provides increased adaptability, innovation, and efficiencies while mitigating risks.

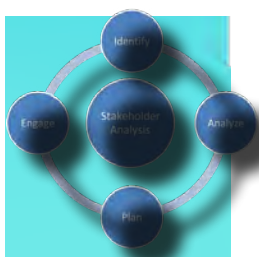
Objective 5.4: Communications, Education and Coordination

Ensure all CBP employees understand their roles in governance to engage in consistent and efficient approaches to compliance across the enterprise

- Role definitions and what they mean
- Everybody understands what makes good governance
- Making governance information available to everyone, such as checklists and points of contact
- Active participation of stakeholders and partners

CBP IT Governance conducts a disciplined process of stakeholder identification, analysis and prioritization as well as development of key communication and training messages targeted to each stakeholder group. Some stakeholder groups only need to be monitored or kept informed, while others need to be actively engaged to be managed closely and kept satisfied.

Careful and intentional management of external and internal stakeholders is a non-negotiable element of strong IT Governance. MGD is composed of integrated divisions that will provide support to all aspects of relationship between CBP OIT, stakeholders, and customers.



- Who are our internal and external stakeholders?
- How does IT Governance affect them?
- What are their roles and how do they influence IT Governance?
- What are the benefits of IT Governance to each stakeholder?
- How to effectively engage and communicate to each Stakeholder?

Acquisition Support

Provide the tools and opportunities to OIT that will enable contract management, acquisition management, and vendor management, and fulfill the advancing equity in federal procurement initiative.

Records and Information Management

CBP Records and Information Management leads and supports creation and preservation of federal records that document CBP’s decisions, actions, and business transactions. effective records and information management is essential to CBP’s success and earning public trust of its actions and integrity.

Program Management

Support program development and capabilities that meet the customer needs, while achieving benefits from standardization and management processes and support policies and legislation.

Workforce Management

Support OIT by recruiting and retaining quality individuals and providing a well-maintained, safe and secure work environment; ensuring workforce wellness and training objectives are met.

Trusted Partnership Initiative

The TPI strategically and tactically delivers IT to operate at the speed of mission, seamlessly, digitally, reliably, and securely.



Organizational Composition of Management and Governance Directorate

Financial Management

Safeguards the financial and physical resources that enable OIT to meet the CBP mission, administers CBP IT Acquisition Review Program, and coordinates with CBP stakeholders to update DHS’ Investment, Evaluation, Submission, and Tracking (INVEST) system to meet requirements of Clinger-Cohen and Federal Information Technology Acquisition Reform Act (FITARA).



CIO BUSINESS OPERATIONS

#6 GOAL

RESULTS-DRIVEN, PEOPLE-FOCUSED: *Customer Experience*

Improve integration of CIO Business Operations services to provide OIT customers with a common, shared user experience to deliver holistic, end-to-end services by collaborating across strategy, budget, acquisition, and workforce activities



[READ MORE](#)

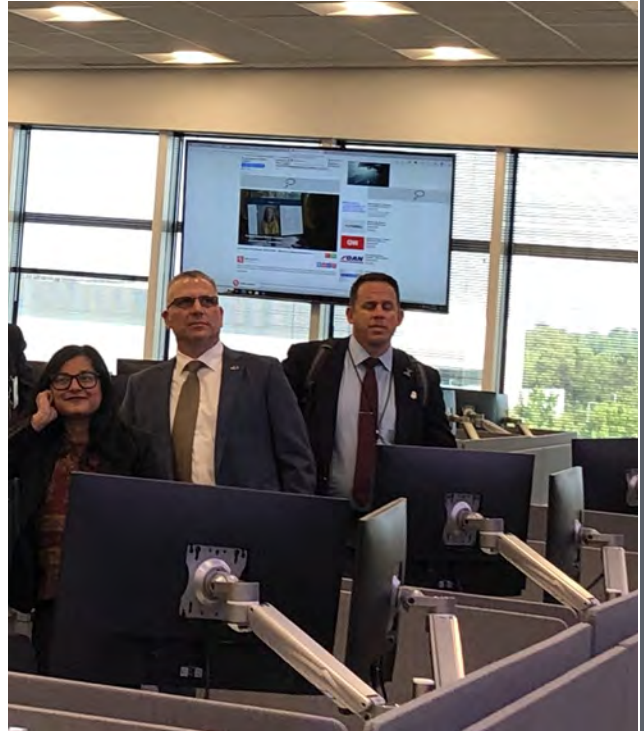
CIO BUSINESS OPERATIONS

RESULTS-DRIVEN, PEOPLE-FOCUSED: *Customer Experience*

GOAL 6: CIO Business Operations

Improve integration of CIO business operations services to provide OIT customers with a common, shared user experience to deliver holistic, end-to-end services by collaborating across strategy, budget, acquisition, and workforce activities

OIT established a MGD to integrate strategy, acquisition, budgeting and workforce functions to improve holistic business services to OIT organizations and our Trusted Partners. OIT's Management and Governance Directorate provides the systems, principles, and processes by which OIT is administered, conducting business with integrity and fairness, to deliver solutions at the speed of the CBP mission.



Success Story:

CBP IT Executive Dashboard

- Developed over 200 dashboards available on any authorized device to provide evidence-based information and analytics to facilitate data-driven decision making
- Cybersecurity dashboard that provides phishing, spillage, patching and capacity information with the ability to drill down to the desired level of detail
- The ACE dashboard contains the availability/health of all 33 ACE application components. Other TPI dashboards for USBP, OFO and OT are well into development

Objective 6.1: Strategy Management

Mature the brokerage of enterprise IT business operations data and information to support evidence-based decision-making by increasing and improving business intelligence capabilities

- Dashboard data quality management and data automation
- Story-driven data visualizations (information) to drive evidence-based decisions
- Additional diagnostic and predictive analytics
- Institutionalized strategy and dashboard adoption to mature decision-making
- Alignment to Federal, DHS, and CBP strategies, plans, policy, guidance, and mandates



Objective 6.2: Cost and Budget Transparency

Instill further rigor and discipline in financial and asset management to get to an informed, balanced budget and asset management strategy

- Reduce quantity and value of must-pay unfunded requests
- Finalize/balance OIT's budget early in the Fiscal Year
- Improve 5-year planning so OIT can live within its budget and establish internal OIT 5-year planning cycle to make Planning, Programming, Budgeting, and Acquisition (PPBA) more "real" within OIT
- Deliver "real" sunset dates for divestiture as well as decisions and annual communications plan

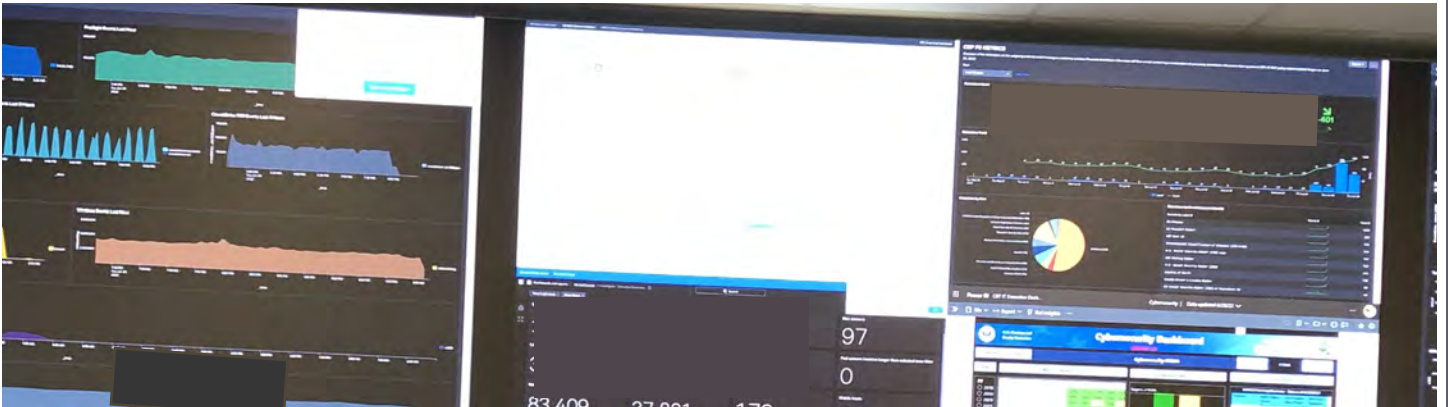
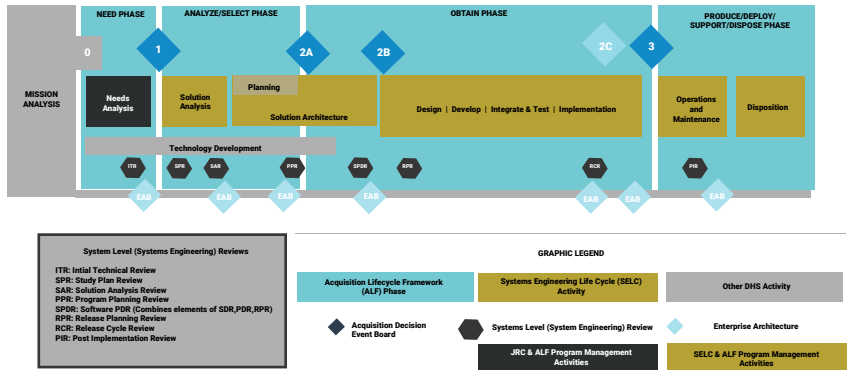




Objective 6.3: Procurement and Acquisition Support

Implement a disciplined approach to requirements definition to improve OIT contract strategies through internal planning, collaboration, and engaging with procurement division early in the acquisition process

- Enhanced dashboard, portfolio, and contract management
- Improved planned acquisition execution
- Right-sized or reduced acquisition footprint
- Appropriately defined contract deliverables

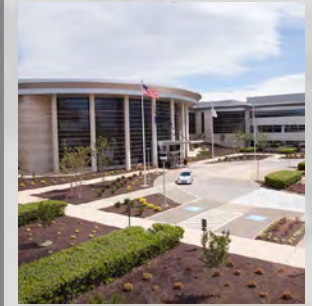
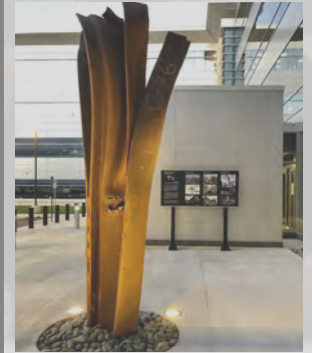
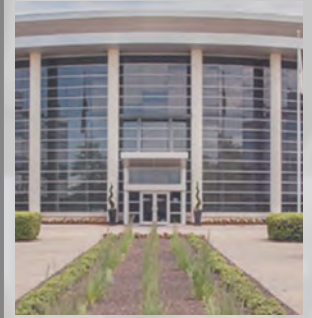
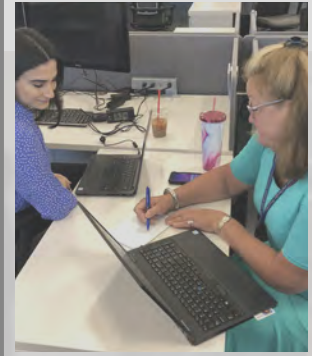


Objective 6.4: Workforce Experience

Enhance employee growth & development opportunities that improve the OIT workforce experience to help employees realize individual career objectives

- Strengthened Employee Resiliency and decrease burnout
- Institutionalized annual career growth and opportunities
- Establish organizational career development framework and culture that enables employees to maximize their potential
- Project “marketplace” concept
- Increased Diversity, Equity, and Inclusion (DE&I) so that all employees “belong”

Increased telework, collaboration tools such as Microsoft Teams, the collaborative environment at the OIT Ashburn campus, and CBP Wellness and Resiliency Programs are examples of initiatives designed to enhance OIT’s Workforce Experience.



WORK LIFE
BALANCE

Objective 6.5: Workforce Management




Strive for a diverse, qualified, and empowered IT workforce to achieve the CBP mission

- Outreach: Recruiting the right people in the right areas from the right populations, as well as diversity in recruiting
- Retention: Workforce experience metrics to support workforce experience
- Money for awards
- Increased employee satisfaction measured through employee satisfaction surveys
- Improved and more integrated processes across budget and workforce
- Streamline the way OIT provides services to employees
- Manage the attrition rate
- Succession planning at the team level
- Increased routine feedback between executives and OIT Workforce Management

OIT's people are its strongest asset. OIT personnel prepare the organization to meet future challenges and take responsible risks that improve CBP's ability to execute the mission. OIT strengthens its technical, leadership, and management skills, and hold ourselves accountable to OIT's values and expectations. OIT workforce management will improve recruiting, retention, workforce processes, and attrition planning. OIT will fine tune outreach to recruit the right people in the right areas from the right populations to increase diversity in recruiting and increase OIT's trend of offers accepted. OIT will improve retention through monetary rewards and responsiveness to employee satisfaction surveys. OIT will increase workforce efficiencies by integrating workforce and budget processes and streamline the way OIT provides services to employees.

CBP OIT Employee Recognition Channels

When you want to...

	 OFFER IN-THE-MOMENT RECOGNITION OR THANKS:	 RECOGNIZE SOMEONE WHO WENT ABOVE AND BEYOND:	 ENCOURAGE SOMEONE WHO HAS A LOT OF POTENTIAL:	 OFFER A PERSONAL NOTE OF THANKS:
PUBLIC	<input type="checkbox"/> During a meeting <input type="checkbox"/> Verbally to their supervisor	<input type="checkbox"/> Nominate them for an award <input type="checkbox"/> Share with OIT leadership <input type="checkbox"/> Send a note to their supervisor <input type="checkbox"/> Submit an OIT Employee Spotlight	<input type="checkbox"/> To develop a new skill <input type="checkbox"/> To take additional responsibilities <input type="checkbox"/> To join a project or work group <input type="checkbox"/> Rotation or detail opportunity	<input type="checkbox"/> Add a standing agenda item for participants to recognize others <input type="checkbox"/> Thank someone on a team email
PRIVATE	<input type="checkbox"/> Send a chat to say "great job" <input type="checkbox"/> Add a note of thanks to an email	<input type="checkbox"/> Separate "job well done" email <input type="checkbox"/> Give a challenge coin or token	<input type="checkbox"/> Remind them of their skills <input type="checkbox"/> Ask about development goals <input type="checkbox"/> Offer to mentor junior staff	<input type="checkbox"/> Send a hand-written thank you <input type="checkbox"/> Stop by to thank them in person <input type="checkbox"/> Schedule video call to say thanks

Measuring and Achieving Success

The goals and objectives within this Strategy must drive OIT actions and collective mindset. To ensure that OIT moves closer to making OIT's vision a reality, OIT has identified specific actions that must be taken to achieve these goals.

OIT has designated a senior leader to sponsor each goal. This leader will be responsible for all implementation efforts associated with that goal and objectives. Every Senior Executive's performance plan will be aligned to OIT's goals and objectives to hold them accountable for the outcome of strategy efforts, and members of OIT must incorporate how they interface with this strategy into their performance plans.

OIT's MGD will establish strategy review mechanisms, facilitate organizational change at all levels, regularly oversee progress of implementation efforts, and serve as a resource for OIT members to propose future strategy enhancements. Additionally, OIT will implement supporting governance and reporting processes and tools, such as the CBP IT Executive and Trusted Partner dashboards, to guide IT strategy management by enabling timely decisions to be made at the appropriate levels.

These tools will contain near real time performance indicators, will maintain line of sight from strategy to measures, and communicate progress to both internal and external stakeholders. OIT will regularly review these indicators internally, with the ITGC, and with OIT Trusted Partners and adjust them to reflect changes and growth happening within OIT and across the CBP enterprise.

Finally, OIT must consistently revisit the strategy itself over the coming years. Success in providing secure, standardized cloud infrastructure and applications for OIT Trusted Partners at the speed of mission will enable us to set even more ambitious goals and objectives.





Deliver secure, reliable IT services and capabilities anywhere, anytime at speed of CBP's 24/7 mission.

CONCLUSION

This strategy charts an aspirational yet achievable course for the future by outlining how OIT will invest in people, infrastructure, and applications, collaborate with ES and trusted partners, and deliver and govern secure, efficient solutions. Delivering on the focus areas detailed in this strategy, along with OIT core operational responsibilities, OIT will anticipate and meet these expectations and continue OIT's critical and integral support of CBP's important mission. This strategy will be a "living plan", continually evolving as OIT implements the objectives within it.

OIT has begun developing detailed plans to advance the goals and objectives in this plan, and these efforts will reach into all levels of the organization. Tapping into the ingenuity and resourcefulness of OIT's entire diverse workforce along the journey through collaborative forums and communication channels will continue to generate strategy implementation ideas from the bottom up.

The U.S. CBP requires a forward-leaning IT organization that enables the nation's premier law enforcement agency to protect the American people and the national economy while safeguarding and managing the United States' air, land, and sea borders. OIT is that organization and will continue to proudly serve the nation.

Strategic Transformation

Tactical Excellence

Innovation

OIT'S STRATEGIC FOCUS AREAS



Mission Infrastructure



Mission Applications



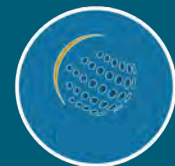
Trusted Partners



Mission Cybersecurity



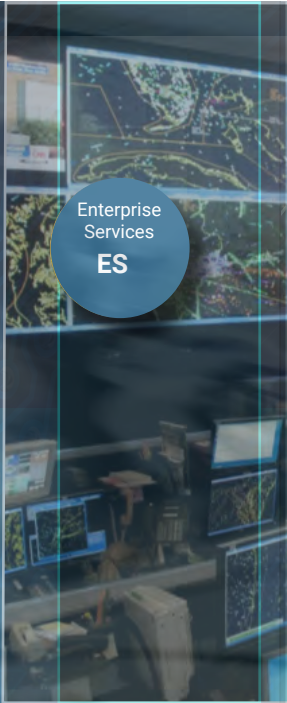
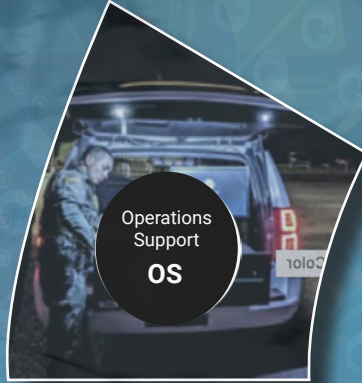
Enterprise IT Governance



CIO Business Operations

OIT MISSION

Deliver secure, reliable IT services and capabilities anywhere, anytime at the speed of CBP's 24/7 mission operations



OFFICE OF INFORMATION AND TECHNOLOGY

