Office of Information & Technology

Traveler Processing and Vetting Software Application Modernization, Development, Enhancements, Operations & Maintenance, and Specialized Services Requirement

May 2019

PERFORMANCE WORK STATEMENT

1.0 BACKGROUND

U.S Customs and Border Protection (CBP) is a component of the Department of Homeland Security (DHS). The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the United States. This important mission calls for improved security at America's borders and ports of entry as well as for extending the zone of security beyond physical borders so that American borders are the last line of defense, not the first. CBP is also responsible for apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; protecting American businesses from theft of their intellectual property; and regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws.

The Office of Information and Technology (OIT) is the information technology component of CBP. OIT's responsibilities are vast-ranging from designing, delivering and maintaining technology based capabilities to enterprise architecture and governance. OIT also provides solutions that support CBP inspection and enforcement activities to help CBP officers, agents, and analysts protect our borders and safeguard America. OIT is responsible for enhancing, administering, and maintaining intelligence and targeting systems and related systems that help secure the supply chain and support CBP's layered defense strategy for international cargo and passengers.

OIT provides application development and continued operational support of traveler and immigration management systems for U. S. Customs and Border Protection. The suite of applications that support traveler and immigration management is called Traveler Processing and Vetting Software (TPVS). TPVS is predominately supported by the Passenger Systems Program Directorate (PSPD) within OIT but other OIT Offices are also involved with TPVS. The PSPD mission is to deliver and sustain technology solutions to prevent terrorism, and safeguard and expedite legitimate travel into and out of the United States. TPVS supports primary and secondary traveler processing at and between U.S. Ports of Entry and vetting services across and beyond DHS. TPVS support a 24X7 mission and handle millions of transactions a day with very quick response times. The CBP mission is very dynamic and the mission requirements evolve as security threats and technologies emerge.

On a typical day, CBP conducts operations at 328 ports of entry within 20 field offices. CBP Officers use TPVS daily to process[1]:

- 1,088,300 passengers and pedestrians
  - 691,549 incoming land travelers
  - 340,444 incoming international air passengers and crew
- 283,664 incoming privately owned vehicles
- 55,709 passengers and crew arriving by ship or boat

[1] Data is from Fiscal year 2017

PSPD has a broad range of stakeholders and users both within and outside of DHS. Figure 1 illustrates major PSPD stakeholders and users.

Figure 1: PSPD Stakeholders and Users

PSPD supports and enhances:

- Port of Entry and related field office and headquarters operations
- CBP Operations including Office of Field Operations, Office of Border Patrol, Office of Air and Marine, Office of Intelligence, etc.
- Lookout Record processing
- Screening across and beyond DHS
- Passenger systems used by the public
- Increased availability of passenger systems
- Architecture guidance and support to standardize systems ensure compliance with CBP/DHS architecture and serves as a path to modernizing passenger systems

2.0 SCOPE

The scope of this Performance Work Statement (PWS) is to procure the full range of life cycle services for CBP PSPD (and potentially other OIT directorates) suite of Traveler Processing and Vetting Software (TPVS) applications and related specialized equipment. Attachment A, Software Application Technical Descriptions and Features, provides detailed information regarding the current applications and services that are in scope. Cloud hosting environments and Software-as-a-Service (SaaS) agreements are under the control of other OIT programs and other contract vehicles for use by applications. The Contractor will be provided Government Furnished Equipment (GFE) operating on CBP networks for TPVS application support services. A common set of development and support tools including SecDevOPS pipeline toolsets are available to the Contractor for use and maintained by CBP. The Contractor may propose new tools for approval by CBP.

Software application services include:

Technology, Modernization, and Cloud Migration
OIT requires TPVS Application Support services that align with CBP OIT's modernization initiatives, one of which is to migrate to the Cloud by 2024. The future of CBP relies on modern technology. To be successful, officers and agents need tailored, intuitive, and advanced capabilities to anticipate and combat emerging threats. CBP's operational environment requires its technology to be innovative, mobile, resilient, available, reliable, and scalable.

Operations & Maintenance Services
OIT requires operations and maintenance (O&M) solutions, processes, and procedures necessary to sustain the suite of software applications and related specialized equipment at the highest levels (as defined in this PWS and referenced documents) of security, service and availability consistent with cost, schedule, and performance objectives. This full range of O&M solutions will ensure computer and TPVS applications operate efficiently, effectively and securely, and are available to support CBP mission requirements.

Development and Enhancements
OIT requires application development, upgrades, updates, modifications and enhancement services with a focus on moving towards a SecDevOps approach. Enhancements include changes to existing applications to meet business or technical requirements. Development may include new applications or major changes to existing applications.

Specialized Equipment
OIT requires a full range of procurement, installation, maintenance, and monitoring, and support services for specialized equipment that supports TPVS applications. The TPVS applications must integrate seamlessly with the specialized equipment.

Project Management and Performance Metrics
OIT requires overall project management support services. Project management is to include oversight, control, and direction in team building, communications, time management, quality assurance and quality control, procedure development, risk management, configuration management, cost management, and software integration.

OIT requires project performance metrics necessary to have visibility into how its application support services are performing in order to effectively manage its application and services portfolio This information will give OIT the ability to baseline, discover trends, identify areas for improvement, and have up-to-date information on the size and scale of all TPVS applications and services.

3.0 APPLICABLE DOCUMENTS

The following documents represent CBP, DHS and other government agency requirements, policies and guidance for which delivery of TPVS application support services must adhere to:

- CBP OIT 2018 Strategic Plan
- DHS Directive 102-01
- CBP Security Policies and Procedures Handbook
- DHS/CBP Program Lifecycle Process Guide
- CBP OIT Agile Governance Framework
- DHS Systems Engineering Life Cycle (SELC)
- CBP SELC process
- CBP SecDevOps Concept of Operations (CONOPS) *(draft)*
- Office on Accessible Systems and Technology (OAST) Compliance
- CBP Section 508 Directive Number 5510-040A

- DHS Information Security Policy, MD4300.1, Information Technology Systems Security
- DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems
- Security Policies and Procedures Handbook HB-1400-05
- All applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series)
- DHS Data Management Policy MD 103-01
- CBP Technical Reference Model (TRM)
- CBP Enterprise Technical Architecture (ETA)
- Federal Data Center Consolidation Initiative FDCCI

These documents are available in a virtual reading room.

4.0 TECHNICAL ENVIRONMENT

Current Environment
OIT performs system activities in a technical environment supported by a broad set of custom architectural components and/or commercial off-the-shelf (COTS) packages. CBP ensures adequate computing capacity for our current and projected needs to include development, testing and production. This includes associated networking, storage and offsite infrastructure.

TECS is a collection of approximately 58 major applications, sub-systems and services with an estimated total of 17.9M Source Lines of Code (SLOC) supporting primary and secondary traveler processing. See Attachment A, Software Application Technical Descriptions and Features, for detailed information regarding each application and service. These applications and services are largely Java based with some additional common technologies. On Premise Applications and services in CBP data centers are primarily deployed as Web application ARchive (WAR) files on Oracle WebLogic application servers hosted on Red Hat Enterprise Linux (RHEL) VMWare ESXi virtual machines. IBM MQ and IBM DataPower Gateway are utilized by software applications. Oracle Exadata database appliances in CBP data centers are the primary data repository.

In addition to WebLogic, some applications are deployed on Tomcat application servers. In addition to RHEL, there are some UNIX and Windows virtual servers. Cloud readiness and planning activities have begun with many of the applications. Some applications, as noted in Attachment A, are already hosted in CBP's AWS Cloud East (CACE). CBP also utilizes cloud-based Software as a Service (SAAS) capabilities such as Salesforce which is used for the eSAFE application. Many applications utilize peripherals such as document readers (chip & MRZ), fingerprint scanners, RFID scanners and cameras (workstation and network). There are no remaining applications operating on a mainframe. OIT does not currently have native mobile applications, however it is considered a growth opportunity.

Future Environment
CBP's vision for primary inspection processing of the future is to transform the way travelers are processed allowing CBP Officers to focus on purpose, intent, and behavior, while maintaining situational awareness rather than concentrating on administrative procedures. A key initiative is to significantly reduce the need for officers to perform data entry and administrative processes wherever technology allows this to be done. The paradigm will evolve from biographic data focused to biometric data centric. CBP will identify travelers biometrically based on information already in CBP holdings as an alternative to having the traveler present their travel document. A biometric-based approach allows threats to be pushed-out further beyond our borders before travelers arrive to the U.S. The elimination of token-based searches as well as the identification of other simplifications of the inspection process will allow for CBP Officers to engage with and focus more on the traveling public. Integration of facial recognition technologies is intended throughout all passenger applications. Additionally, CBP's vision is to transition frontline officers from static booths, to a dynamic and agile operation allowing officers to admit or refer travelers using mobile technology with a single touch point. In addition, CBP envisions expanded use of public facing self-service web-based and native mobile applications by travelers in all stages of the travel

process.

OIT's future environment is in alignment with CBP's modernization initiatives. The future of CBP relies on cutting-edge, modern technology to be successful and officers and agents need tailored, intuitive, and advanced capabilities to anticipate and combat emerging threats. CBP's operational environment requires its technology to be innovative, mobile, resilient, available, reliable, and scalable. Furthermore, rapid delivery of enabling technologies such as cloud computing, edge computing (data processed where it is generated), automation, and artificial intelligence offer potential leaps of performance and utility. CBP OIT's primary modernization goals are:

Resiliency and Recovery Identify, prioritize and address challenges within existing mission critical systems to immediately reduce and quickly recover from outages.

Mobility and Application Development Expand the use of leading practice application development across offices with like customer needs to achieve rapid, continuous, and secure deployment of new capabilities to all platforms, readily providing mission-required functionality to agents and officers in the field.

Analytics Support an enterprise-wide data management strategy to make readily available anytime and anywhere across the enterprise, delivering tools and datasets to further data-driven mission performance into operators' hands. Note: Data analytic services are outside the scope of OIT. However, OIT captures data that is used for analytics.

Cloud and Infrastructure Develop an integrated cloud migration and infrastructure modernization action plan for all mission essential systems and mission relevant systems, delivering modernized capabilities (e.g., disaster recovery and high availability) and improved user interfaces with no interruption in service. Additionally, continue to enhance CBP's cybersecurity posture in support of both cloud migration and increased edge-device use without impacting system effectiveness.

5.0 OPERATING ENVIRONMENT REQUIREMENTS

5.1 OIT solutions must use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP Technical Reference Model (TRM). If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process. The DHS/CBP TRM will be updated as technology insertions are accomplished.

5.2 OIT systems must adhere to the CBP Enterprise Technical Architecture (ETA). The ETA establishes a consistent, vendor-agnostic, standards-based architecture to be used by CBP in the development of modernized application systems.

5.3 All Application O&M and maintenance, updates, enhancements, upgrades, or modifications solutions within the scope of this PWS are inherent to the TPVS applications and the corresponding application infrastructure. The platforms on which the TPVS applications operate (National Data Center, DHS Data Center, and CBP AWS Cloud Environment (CACE)) are under the control of other OIT programs and other contract vehicles, however TPVS application teams must support infrastructure maintenance to ensure it does not impact the TPVS applications. Software changes are required to continue to properly interface with host platforms and existing physical and software interfaces. As infrastructure and applications are modernized and migrated to and operated in the cloud, the TPVS applications must continue to meet or exceed their system performance (measured in response time, availability, and scalability) prior to the modernization and/or migration effort. TPVS applications must meet or exceed their required security posture while operating in the cloud.

5.4 All proposed enhancements, improvements, modernizations and new capabilities added to systems are subject to review and approval by the Government in accordance with their Configuration Management/Control Plans.

5.5 All systems are subject to 508 compliance per CBP Section 508 Directive Number 5510-040A.

5.6 All personnel supporting OIT must have proper DHS/CBP security clearances per the CBP Security Policies and Procedures Handbook.

5.7 All contractor personnel supporting work on this PWS are required to use GFE computers and software hosting facilities. Exceptions must be approved on a case-by-case basis by the COR.

5.8 All TPVS applications and the work in an environment that requires collaboration and cooperation with other government agencies and other contractors supporting OIT and other related programs with common or shared missions and objectives.

6.0 OBJECTIVES

The overall objective is to obtain the full range of operations and maintenance support for the suite of TPVS applications and associated specialized equipment as identified in the following objectives. This includes ensuring TPVS applications and specialized equipment are properly developed, maintained, updated, and enhanced as necessary to support the critical and dynamic mission requirements of the CBP. These objectives are all equally important to CBP.

A Quality Assurance Surveillance Plan (QASP) will be created for each individual task order issued against this BPA award. The QASP will include metrics, performance standards and acceptable quality levels for achieving the objectives of the individual task order.

Objective 1: Proactive Operations & Maintenance

CBP relies upon TPVS applications and services for mission critical primary and secondary traveler processing at and between U.S. Ports of Entry and vetting services across and beyond DHS. This objective is to proactively provide all operations and maintenance (O&M) solutions, processes, and procedures necessary to sustain the suite of deployed TPVS applications, services and specialized equipment at their peak efficiency while maintaining an up-to-date security posture, maximizing resiliency, and minimizing issues and/or downtime. Each TPVS application and service has its performance, availability, and security requirements which define its peak efficiency. See Attachment A, PSPD Software Application Technical Descriptions and Features, for specific performance, availability and security requirements.

OIT requires a full range of O&M solutions that are necessary to ensure TPVS applications, services and specialized equipment operate efficiently, effectively and securely, and are available to support CBP mission per their individual requirements. OIT requires proactive preventive and perfective maintenance while minimizing the need for reactive corrective maintenance necessary for resolving service disruptions.

The proactive approach to operations and maintenance of TPVS applications should provide the highest levels of service and availability through a comprehensive maintenance methodology to optimize performance capability, minimize costs, and effectively manage performance risks. Proactive O&M is a centralized capability. Occasional temporary travel may be required to support fielded systems.

<u>Systems Performance Monitoring</u>
O&M support includes monitoring the health and performance of production TPVS applications and all associated specialized hardware, troubleshooting software, troubleshooting specialized hardware, fixing software defects, repairing or replacing specialized hardware, as well as designing, creating, testing and

implementing software production baseline updates. OIT requires performance monitoring tool a n d expertise by the Contractor to consult, configure, develop and operate effective performance monitoring services.

OIT requires a real-time, centralized system dashboard capability to monitor the performance, configuration, status and health of all fielded systems. This capability will provide the overall health of all operational systems and allow for issues encountered to be discovered and remedied proactively without CBP operational personnel knowledge or involvement. Maintenance actions by the Contractor are to be coordinated with the CBP Level I Help Desk, which is operated by the CBP ENTS Directorate, and with the Field Support Directorate. A centralized systems performance monitoring dashboard for TPVS applications is a new capability.

O&M support will emphasize proactive performance monitoring to identify and resolve performance risks before they impact mission achievement while responding to customer identified performance deficiencies and/or outages. System performance is to be evaluated on a continual basis to ensure there is no degradation to current performance levels as system capabilities and usage continue to grow. Each T P V S application and service has its performance and availability requirements which define its peak efficiency. See Attachment A, PSPD Software Application Technical Descriptions and Features, for specific performance and availability requirements.

OIT requires Contractor support for disaster recovery exercises for TPVS applications. "Table Top" exercises, where processes are walked through without actually failing over, are performed quarterly. Disaster recovery exercises with systems failing over to the DR site are performed twice a year.

Production Monitoring Support

OIT requires a U.S.-based Tier II and III production monitoring support capability with 24x7 telephonic availability and on call maintenance support to respond to corrective maintenance issues working in coordination with the CBP Enterprise Operations Center (EOC) Technology Service Desk and production monitoring teams. The Contractor will participate in ad hoc production support requests initiated by the T P V S CBP EOC to assist in troubleshooting and resolving issues. The Contractor is responsible for resolving T P V S application and specialized equipment integration issues. When necessary, the Contractor provides support to Infrastructure teams and interfacing TPVS application teams for troubleshooting and resolving issues impacting TPVS applications. Given the mission critical nature of TPVS applications, production issues are expected to be resolved as soon n as possible.

Tier II support consist of qualified technical professionals with the ability to effectively troubleshoot, diagnose, and correct or resolve software and hardware problems. Tier II capabilities includes the ability to diagnose and correct problems by interpreting system, application, and database log file information.

Tier III support consist of qualified technical professional subject matter experts (SMEs) who can provide software and hardware expertise to a Tier II technician if that assistance is deemed necessary. Tier III SMEs are to have the technical knowledge necessary to assist the Tier II technician on software and hardware issues that are outside of the normal problems.

On-site support in response to a tier II and / or tier III issue may require a qualified field maintenance technician to be physically available at the facility to ensure that the issue is resolved in a timely manner. The Government takes the lead for coordination and outreach for maintenance of onsite systems and equipment with the POE Port Director, and the POE Field Technology Officer (FTO) via the OIT Field Support Area Manager to avoid or minimize operational disruptions. If necessary, a Tier III SME may be expected to lend assistance on site, in cases where his/her presence is required. Tier III SMEs are expected to work with site FTOs when necessary.

Development & Integration Testing

OIT requires development and integration testing services to be conducted in an automated manner throughout the software application support process of all TPVS applications, services, and specialized equipment to assist in engineering design and development and to verify that technical performance specifications have been met. Development & Integration testing capabilities shall support the proactive

operations & maintenance objective, as well the enhancements & modernization and new development and emerging technology objectives requiring specialized equipment to enhance capabilities of TPVS applications. Automated testing processes following CBP's SecDevOps approach is a key objective to support agile rapid application development and for improved system quality. Development & integration testing is conducted by the Contractor and includes testing of components, subsystems, preplanned product improvement changes, hardware/software integration, and production qualification testing. It encompass the use of SecDevOps automated test tools, models, simulations, test beds, and prototypes or full-scale engineering development models of the system. Development & Integration testing services support test-driven development activities.

Objective 2: Enhancements & Modernization

OIT requires TPVS application enhancement and modernization services in order to:

- Quickly provide increased functionality in a secure and stable manner.
- Move all TPVS applications out of CBP's National Data Center (NDC) and into the cloud or alternative hybrid solutions by 2024.

Enhancements

Enhancement services are the modification of software applications performed after delivery into production to keep the TPVS application useable in a changing environment. Enhancements address ongoing mission needs for new functionality, collection of additional data, and implementation of new system-to- system interfaces, enhancements to existing interfaces, etc. This effort encompasses system upgrades and improvements, which are generally updates/changes to existing systems and the corresponding infrastructure installation, patching, and management. A key enhancement objective is to identify and incorporate software solutions to optimize the performance and operational cost efficiency of the suite of computer and TPVS applications in support of the CBP mission.

Enhancement services include all phases of software requirements, design, development, testing and implementation, to ensure TPVS applications continue enabling their users to meet their mission goals and objectives. These efforts include the full range of software requirements, including planning, requirements definition and analysis, systems design and development, coding and testing, integration, implementation and production support, and legacy system retirement.

Any TPVS application upgrades, enhancements or modifications, will be reviewed and approved in accordance with the CBP change management process, and performed and documented in accordance with CBP and DHS Systems Engineering Life Cycle (SELC) tailored for agile development processes and rapid releases.

Modernization

OIT is a large portfolio of mission critical passenger and immigration management systems in all different phases of the application lifecycle from legacy systems nearing end-of-life to newly released development. Modernization addresses the migration of legacy to new applications or platforms, including the integration of new and improved functionality. Modernization objectives supports CBP's cloud migration objective by re-engineering applications to benefit from cloud hosting capabilities for rapid provisioning and scaling. This objective is to identify, plan, and implement modernization activities throughout the TPVS application portfolio. Modernization efforts may be major system overhaul projects as well as re-engineering efforts (such as code containerization) embedded within the everyday enhancement and O&M work. When TPVS applications are touched, changes are to adhere to CBP's most recent architecture roadmap where possible to incrementally modernize applications.

Cloud Hosting

The CBP OIT Data Center Migration (DCM) effort is moving all TPVS applications and services out of the NDC and to the cloud by 2024. As part of CBP's DCM effort, OIT requires cloud modernization and cloud migration expertise and services for TPVS applications to be hosted in the cloud in a cost-effective,

secure, and agile way. Each TPVS application, whether legacy or new, will require analysis and planning for the optimal modernization or migration strategy to move into the cloud. An application's strategy may involve interim steps to insure continued operations and for alignment with external dependencies. In addition to the applications, each supporting TPVS application database will require analysis and planning for the optimal modernization or migration strategy for moving data into the cloud. This includes participating in data assessment and consolidation efforts to reduce redundant data across all CBP Directorates. In cases where cloud hosting is not feasible, OIT requires alternative solutions for moving solutions out of the NDC.

The strategy for cloud based services and infrastructure should align to the strategy of the Federal Data Center Consolidation Initiative (FDCCI), the objectives of the enterprise service delivery model, the CBP OIT target/cloud architecture, and support the agency's ability to deliver future sustainable services. This effort will enable OIT to innovate and modernize the way software is built, deployed and managed. The approach will need to successfully enable OIT to quickly, reliably and consistently deliver modernized digital solutions moving forward. Cloud modernization includes building digital solutions based on micro services, implementing API based modern web frameworks, building TPVS applications that are extensible to mobile and forward-looking industry paradigms, building consistent, standard, reliable and portable environments in the cloud, and defining container strategies and operational models. Cloud migration support includes conducting an inventory (including users, applications, infrastructure, security and privacy, and service management), application mapping, conducting suitability analyses, providing recommendations to the government for the industry/service model, migration planning, including developing the migration roadmap, maintaining cloud infrastructure servers and virtual servers, operating systems, databases, applications containers and associated software, patching, DNS, network, storage and message transport.

OIT requires support for cloud Software-as-a-Service (SaaS) applications. CBP currently utilizes Salesforce as a Customer Relationship Management (CRM) tool for the eSAFE application. Support includes providing tool subject matter expertise, configuration, development, administration, and operations & maintenance.

SecDevOps

OIT requires all TPVS application support work to follow CBP's SecDevOps processes as identified in the CBP SecDevOps Concept of Operations and utilize its Continuous Integration and Continuous Delivery (CI/CD) pipeline toolset for improved quality and process efficiencies. CBP has enabled a DevOps pipeline that leverages a common code repository to rapidly develop and deploy new software capabilities. CBP's SecDevOps Plan integrates security throughout the development lifecycle pipeline so that it is transparent and just not seen as a gate prior to deployment. CBP's CI/CD pipeline begins with a common source code repository for all applications and provides a shared set of automated build, test, QA, security, and deployment tools. Along with an enhanced security process objective, automated testing is also a key objective for OIT to realize improved quality, faster release cycles, and more efficient use of testing resources. Current CBP CI/CD pipeline tools include Gitlab, Jenkins, Black Duck, SonarQube, Se, Docker, Artifactory, JFrog XRay, Aqua, and Open Shift or DC/OS. These tools are managed by CBP EDME for use by OIT and other CBP application directorates. The CI/CD pipeline is targeted for applications implemented in the cloud including applications hosted in CBP's on premise cloud environments. Contractors may propose changes to CBP's SecDevOps processes and CI/CD pipeline tools for consideration.

Objective 3: New Development and Emerging Technology

OIT requires new development services in order to quickly develop new TPVS applications based on world events, stakeholder requests, and technological advances recognizing that OIT always has new hot projects with challenging schedules and often these projects are not on the known horizon of work. New development services include all phases of software requirements, design, development, testing, and implementation to ensure TPVS applications will enable its users to more effectively meet their CBP mission goals and objectives and take advantage of the latest advances in technology.

These efforts include the full range of software design, Test-Driven Development (TDD), implementation

and integration, including planning, requirements definition and analysis, systems design and development, coding and automated testing, production, implementation, integration, and TPVS application maintenance. This effort encompasses new TPVS application development (for web-based, native mobile, and potentially other application platforms) and system modernization projects. New development is to follow CBP's Agile Framework and DHS SELC procedures tailored for agile development as well as CBP's SecDevOps processes. CBP currently follows the Scaled Agile Framework (SAFe) model with two week sprint cycles for all development activities. Travel may be required to ports of entry in support of initial deployments of newly developed functionality.

Objective 4: Specialized Equipment

OIT requires full range of hardware O&M support for specialized equipment to support end-to-end operations of OIT systems. Specialized equipment services include operations, maintenance (i.e. tune, repair, replace), monitoring, procurement and installation services for specialized equipment such as kiosks, jump kits, portable systems, accessories, camera systems, biometric capture devices and software, document readers, document authenticators, and telecommunication devices.

Specialized equipment is subject to change over the period of performance based upon new requirements and emerging technologies.

The key to successfully supporting specialized hardware is to ensure that effective monitoring of the equipment is implemented and that logging and tracking of operational issues is performed to proactively identify where the greatest risk of hardware failures exists and allow for predictive maintenance schedules to be developed. When scheduled maintenance is performed, as opposed to reacting to failures, continuity of operations will be maintained, impacts to users minimized, and customer satisfaction increased.

Specialized equipment services include tracking detailed information on OIT equipment as part of the CBP technology overview plan. Up-to-date information on government hardware is to be maintained, including fielding and maintenance status, warranty, location, Points of Contact responsible for operation and sustainment of the equipment, pertinent help desk tickets and information on service performed.

OIT requires to improve its ability to predict equipment lifecycles and schedule maintenance in advance of failure and minimize impact to operations. This includes analysis of hard data such as Mean Time between Failure (MTBF) and Mean Time to Repair (MTTR) for each type of hardware to identify trouble prone items and consider remedial actions.

Items of specialized equipment currently include, but are not limited to, the Global Entry kiosks, Global Enrollment System jump-kits, camera systems, biometric capture devices, document readers, document authenticators, telecommunications equipment, and removable media. Support includes replacing existing inventory or adding to inventory as directed by the COR.

Objective 5: Collaboration

OIT requires a collaborative environment where the Contractor effectively works with other CBP, DHS, other Government Agencies, and commercial organizations including other contractors. CBP's mission achievement is dependent on effective collaboration by the many internal and external organizations. OIT is committed to CBP's "One OIT" goal as described in the CBP OIT 2018 Strategic Plan with the objective of operating as a single transparent organization with a unified mission focused culture. A highly-collaborative environment will foster the sharing of information, resources, best practices, and opportunities to streamline processes across all of OIT. OIT requires a Contractor committed to the "One OIT" mindset.

Objective 6: Innovation & Thought Leadership

OIT requires thought leadership on using innovation, new technologies, new methods, new ideas, new efficiencies, etc. to improve OIT support for the CBP mission. OIT is looking to instill a culture of

innovation into all TPVS application support activities. OIT provides CBP, DHS, and stakeholder enforcement agencies the data they need, when they need it, to support and accomplish the important mission of protecting travelers, trade, and the homeland. Innovation and constant improvement is paramount to deliver and sustain technology solutions that ensure the safety and security of travelers entering and exiting the United States, while facilitating and streamlining legitimate trade and travel. Innovation is to be continuous and based on the following approach pillars:

- Innovate to reduce cost
- Innovate to improve service/performance/resilience
- Innovate for end-point customer service
- Innovate to improve delivery speed and quality

OIT requires support to identify new, innovative ways of enabling more effective and efficient performance. This objective is to be used as a means for improvement and possible replacement of existing TPVS applications and processes. OIT requires innovation in, but not limited to, the following areas: surge capacity, increased consistency and value of applications, improved quality, improved user experience, reduced project risks, reduced re-work, reduced implementation and O&M costs. OIT's vision is to continue to streamline operations by introducing efficiencies.

OIT requires an overall architecture support capability to provide Enterprise Architecture guidance, technology roadmap services, technical tool support, and overall innovation support to all TPVS application teams. The architecture support team will work closely with CBP OIT's Enterprise Architecture Branch and coordinate with all TPVS application teams.

Innovation and thought leadership is to be infused into all software development, modernization, enhancements and steady state operations activities.

Objective 7: Holistic Project Management

OIT requires project management services to manage TPVS applications from a holistic perspective understanding the dependencies between all of the applications and opportunities to work efficiently and effectively across the portfolio. The contractor shall provide management expertise, oversight, control, and direction in team building, communications, time management, quality assurance and quality control, procedure development, risk management, configuration management, cost management, and software integration.

An Agile-based, holistic approach to project management is critical to CBP's mission as it provides enhanced visibility throughout the lifecycle of a project, enabling the necessary insight into achievement, progress, challenges, goals and next steps. It also enables OIT to accommodate high priority changes and changes in direction as dictated by the product owners and the user community, in response to new and evolving threats and risks. OIT is a very agile, nimble organization and new features which comply with the user requirements are often implemented in a very short amount of time. In an Agile organization, project teams deploy functionality incrementally, minimizing the potential for risk impacts, and provide streamlined documentation throughout the phases of a project. The Contractor is expected to do sprint and release planning (i.e. with user stories in Jira), execution, review and demonstration and retrospectives. The Contractor will determine, prioritize, and document the product backlog for the project, develop definitions of done, conduct daily scrums, and utilize CBP tools to document the agile process.

OIT requires t proper staffing and skill set coverage at all times. The Contractor shall have the ability to recruit, hire, and retain CBP-cleared resources and effectively address changes in work priorities and staffing.

The contractor shall provide project management services which includes transition planning, project planning, scheduling, tracking, and overall financial management. Specific support requirements include the preparation of plans and schedules based on technical and management data; scheduling and conducting technical and planning meetings; conducting reviews; and preparing status reports.

The Contractor will provide support for Integrated Product Teams (IPTs) as directed by the Government in support of the development/deployment of future functionality. The Contractor will work with the IPTs to ensure alignment and compliance between deliverables, schedule, scope and agile methodologies. The Contractor will also support the Government IPT project manager with Agile support and provide regular status reporting and scheduling that complements the Agile development methodology.

The Contractor will conduct weekly status meetings to discuss status of projects, issues, and problem areas related to the projects. The results of each meeting are to be documented and submitted to the Government. In addition to reporting the status of each project, fund status reports are to be provided to the Government. The Contractor shall conduct oral presentations and/or executive briefings on the project and TPVS application statuses when necessary.

Agile project management methodology must follow the DHS SELC tailored for an agile approach for rapid development and comply with CBP and DHS policy. The Contractor shall assist OIT with the CBP acquisition process when necessary following DHS Directive 102-01.

Objective 8: Project Visibility

OIT requires project visibility on all activities, costs, performance, risks, etc. This includes meaningful reporting that provides OIT with up-to-date and comprehensive information regarding technical and management performance. Project visibility will increase and enhance collaboration, responsiveness, transparency, and accountability with business owners and stakeholders, to ensure end users/stakeholders receive a high level of customer service to address high priority requests timely and to deliver new and enhanced solutions quickly, according to priorities set by the stakeholders.

Performance Metrics

OIT requires the information required to have visibility into how its TPVS application support services are performing in order to effectively manage its application and services portfolio This information will give OIT the ability to baseline, discover trends, identify areas for improvement, and have updated information on the size and scale of all TPVS applications and services. Performance metrics may include agile process metrics, production metrics, security metrics, size-oriented metrics, and function oriented metrics. Agile process metrics measure the effectiveness of the system change process from idea to deployment. Production metrics measure the efficiency of the development process. Security metrics measure the effectiveness of security incident remediation. Size-oriented metrics measure the size of supported applications. Function-oriented metrics measure defects and defect removal efficiency. OIT requires the types of metrics that are all vital for effective management of the TPVS application portfolio support services activities.

Project Management Dashboard

OIT requires to have a Project Management Dashboard capability accessible on the CBP network to monitor the overall performance and progress of work within the scope of this PWS to track schedule, costs, workload, risks, and issues of the project delivery teams. The dashboard will provide at-a- glance data and metrics about the current status of the performance of all project teams and allow for more detailed views of individual project teams. The dashboard is to be a configurable solution to display information pertinent to individual project teams.

7.0 DELIVERABLES AND DELIVERY SCHEDULE

Deliverable ID	Description of Deliverable	Deliverable Date/Time Frame
0001	Security Plan	No later than 5 days following contract award
0002	Incoming Transition Plan	Due with Phase II response
0003	Submission of all CBP BI Packages	No later than 5 days following contract award
0004	Post-Award Kick-off Meeting	No later than 5 days following contract award
0005	Weekly Status Reports and Meetings	Weekly
0006	Contract Staff Training Requirements	As Required; To be reported by the 1st and 15th day of each month.
0007	Ad-hoc reports	As Required
0008	Project Management and SELC Documentation	As Required
0009	Out-Going Transition Plan	180 days prior to the end of the final period of performance

7.1 Security Plan

The contractor will be responsible for ensuring that the contractor team complies with contract security requirements and sensitive information protection policies, including ensuring that all personnel have the appropriate level of clearances. The contractor will deliver an IT Security plan to the Government outlining their plan to comply with the Government's administrative, physical and technical security controls in accordance with the terms and conditions in Attachment 4.

7.2 Transition Plan

The incoming transition period begins on date of award and runs for the next 180 calendar days. The outgoing transition commences 180 days prior to the end of the final period of performance. The Contractor shall submit a Transition Plan that captures the Incoming Transition Period (Transition-In Plan). The Contractor is fully responsible or all aspects of the work throughout the Incoming Transition period in accordance with the Contractor's Transition-In Plan. The Contractor shall make all necessary preparations to begin performance in accordance with its Incoming Transition Plan in order to ensure no impact to daily operations or scheduled critical activities.

An Outgoing-Transition Plan shall be delivered 180 calendar days prior to the BPA expiration date unless otherwise directed by the CO. The Contractor shall account for a 10 business day Government review process prior to executing the transition. Upon award of a follow-on contract, the incumbent Contractor will work with the new Contractor to provide knowledge transfer and transition support, as required by the COR.

The DHS CIO has established portfolio targets for the IT infrastructure that include production system consolidation at a DHS data center, and transition to OneNet. The contractor must be prepared to support CBP government leads, within the purview of this BPA, to provide any required transition planning or program execution, associated with meeting the transition timeline. Transition activities may include:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

7.3 Weekly Status Reports

The contractor will provide regular communication of project status through weekly status reports and weekly face-to-face status meetings between the team, the COR, the CBP government leads and any other stakeholders as identified by the Government. The contractor is responsible for monitoring the contract by tracking expended funds.

The Contractor shall provide the COR with a weekly report, for each objective in section 6.0 with an overview of work accomplished the previous period and work scheduled for the upcoming week. This report shall contain the following information at a minimum:

- Planned activities and desired results for the next reporting period with milestones and deliverables;
- Issues and risks affecting technical, schedule, or cost elements of the contract, including background, impact and recommendations for resolution;
- Results related to previously identified problem areas with conclusions and recommendations;
- Team organizational chart;
- Monthly update call protocols in event of system issues as well as name/emails/phone numbers applicable to parties involved (Prime/Sub/Gov't).
- Funds Status Report that supplies funding data about the BPA.
    - Updating and forecasting contract funds requirements based on burn rates;
    - Developing funds requirements and estimates in support of approved investments;
    - Determining funds in excess of contract needs and available for de-obligation.

7.4 Contractor Staff Training

All contract personnel are required to complete the DHS/CBP mandatory PALMS training courses by the mandatory due date(s). The Contractor is responsible for maintaining records of contracting employees that have completed the mandatory training and provide semimonthly updates to the COR on the 1st and 15th day of each month or the next business day if the 1st or 15th is a Holiday or on the weekend. The Contractor is also responsible for providing copies of the training certificates to the COR when requested.

8.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

(a) The Government will furnish only that equipment necessary for the Contractor to carry out its work efforts under this PWS at the Government facility. This includes normal workspace accommodations such as desk, chair, desk phone, and computer. While performing work under this PWS in Government facilities, the Contractor may have the use of other normal office EIT devices, such as fax machines (not classified), copiers, projectors, etc. It is required that the contractor obtain CBP Personal Identity Verification (PIV) cards as they are necessary to log into all computers and laptops.

(b) The Government will provide to the Contractor cell phone, laptop, or other portable devices, such as mobile devices or other PDAs upon the written consent of the COR justifying the need for such equipment.

(c)) The Government will furnish all necessary related documentation in its possession that may be required for the Contractor to perform this contract.

9.0 SKILL MIX

The Contractor shall provide personnel with the requisite experience in the tools, methodologies and protocols specified in this PWS, as well as all technologies in the Technology Reference Model (TRM), currently or as they are added to the TRM. OIT requires the Contractor to support their technical solution with highly-educated, highly-skilled and highly-experienced contractor staff in order meet the objectives.

This following is a characterization of the breadth and scope of skills that CBP requires within this PWS.

1) CBP has high volume, high performance, and real-time applications operating in an environment that requires specialized, demonstrated management and technical expertise, as well as personnel able to successfully obtain a CBP/DHS background investigation. As the systems managed under this contract play a key role in carrying out the CBP mission, CBP places more value on specialized and demonstrated experience for support staff performing in support of this PWS.
2) The Contractor shall provide certified, trained, and knowledgeable technical personnel according to the requirements of this contract. Therefore, CBP will not provide or pay for training, conferences, or seminars to be given to contractor personnel in order for them to perform their tasks. The contractor will also not be able to charge hours to the Government while attending said training, conferences, or seminars. If it is determined during the performance of the contract that training, conferences, or seminars not specified in the contract are required, only the CBP Contracting Officer may approve the training.
3) The Contractor shall provide the full range of test validation, verification, and evaluation solutions to ensure that all IT products and services meet DHS standards, and are performing to defined design, cost, schedule and performance specifications /capabilities. The Contractor shall work with the Government to propose new tools and software for testing, verification, and evaluation if necessary.

The Contractor shall adequately manage its staff and plan, direct, control, measure, and monitor all employee activities. The Contractor shall ensure processes for recruiting, training, retaining, advancing, cross-training, supervision of, managing, interfacing with the Government, , and that processes incorporate obtaining timely security clearances for new employees.

10.0 PERIOD AND PLACE OF PERFORMANCE AND HOURS OF OPERATION

10.1 Period of Performance

This work will be performed on a Time and Material basis with a twelve (12) month base period, plus four twelve (12) month option periods. The period of performance will include a 180-day Transition Period within the base year:

Base Year: December 2019 – December 2020
Option Year 1: December 2020 – December 2021
Option Year 2: December 2021 – December 2022
Option Year 3: December 2022 – December 2023
Option Year 4: December 2023 – December 2024
Option to Extend Services Period: December 2024 - May 2025

10.2 Place of Performance

U.S. Customs and Border Protection (CBP) will provide space in multiple facilities for the on-site contractor staff to perform the required tasks in the Washington DC Metro area, however most work is performed at the sites below. Note that the location will shift to Ashburn VA when OIT moves there in

2020. Current locations for this work are below, although other Washington DC area offices may be occasionally used. All work required under this contract shall be performed by the Contractor at Government sites and/or Contractor provided facilities for staff where Government Facilities cannot accommodate. Travel to other Washington DC area Government locations may be necessary.

a. NDC 3, 7400 Fullerton Rd, Springfield VA 20598
b. Bostons Building, 7375 Boston Blvd, Springfield VA 22153
c. 10720 Richmond Hwy, Lorton, VA 22079
d. 7799 Leesburg Pike, Falls Church, VA 20598
e. Beauregard Facility, 1801 N Beauregard St., Alexandria, VA 22311
f. Quantum Park, 22001 Loudoun County Pkwy, Ashburn, VA 20147

10.3 Hours of Operation

For those contractor personnel working in direct support of OIT, the normal business hours are 7:00 am to 6:00 pm (EST), Monday through Friday with core business hours between 9:00 am and 3:00 pm each business day. The contractor shall ensure coverage of these core hours for those in direct support of the OIT. OIT and those directly supporting OIT will recognize all official federal holidays. However, all computer and software applications support a 24/7/365 mission requirement and the contractor shall ensure system TPVS application performance standards are maintained over the full range of mission operations. Due to the nature of the work, overtime is authorized, however all overtime must be requested in advance and approved by the COR. The Contractor must provide a central point of contact to reach the necessary staff in the event of system problems or emergencies. If required by the COR or Government Team Lead, the contractor's staff shall report on- site after normal hours to address system problems.

11.0 TRAVEL

For any remote to be authorized, the contractor must submit the request for travel to the COR in advance to the travel being taken. The request for travel must be approved, in writing, by the COR prior to travel.

Travel expenses shall be separately identified on invoices accompanied by all approvals and paid receipts during the time of travel.

Local travel will not be reimbursed if the contractor has an assigned workstation at a location.
The following approvals must be obtained in writing in advance of the trip.

International: Government Director, COR, Executive Director
Domestic: Government Director, COR,
Local: Government Director, COR

Section 12.0 thru the end of Page 38 should move to Attachment 4 T's and C's. Except the 2 HSAR clauses; they can go with Clauses

12.0 CONTRACTING OFFICER AND CONTRACTING OFFICER'S REPRESENTATIVE

Notwithstanding the contractor's responsibility for management during performance, the administration of this BPA will require coordination between the CBP and the contractor. The Contracting Officer (CO) will appoint a Contracting Officer's Representative (COR) to assure orderly performance of the tasks and provide technical direction. The CO and COR are:

Contracting Officer (CO):

Name:	Sharon Hallinan
Telephone:	202-556-6604
Email:	sharon.e.hallinan@cbp.dhs.gov

Contracting Specialist (CS):

Name: David Seay
Telephone: 202-344-3482
Email: david.seay@cbp.dhs.gov

Contracting Officer's Representative (COR):

Name: Michelle Nelson
Telephone: 571-468-5908
Email: michelle.nelson@cbp.dhs.gov

The types of actions within the purview of the COR's authority are to assure that the contractor performs the technical requirements of the order; to perform or cause to be performed inspections necessary in connection with performance of the order; to maintain both written and oral communications with the contractor concerning the aspects of the order within his/her purview; to issue interpretations of technical requirements; to monitor the contractor's performance under the BPA and notify the contractor and CO of any deficiencies observed; and to coordinate Government-Furnished Property or Data availability and provide for site entry of contractor personnel if required.

The COR will provide no supervision to contractor personnel. The COR is not empowered to make any commitments or changes which affect the BPA pricing or other items and conditions. Any such proposed changes must be brought to the immediate attention of the CO for action. The acceptance of any changes by the contractor without specific approval and written consent of the CO shall be at the contractor's risk.

PWS Attachment A

Software Application Technical Descriptions and Features

Table of Contents

Advance Passenger Information System (APIS)

Advanced Passenger Information System (APIS) – Inspection Processes Division			
The Advanced Passenger Information System (APIS) is an external service and an internal application used to review air, sea, train, and limited bus passengers and crew in an effort to identify possible terrorists, uncover high-risk individuals, and facilitate the clearance process for legitimate travelers. APIS supports CBP mission delivery by screening the information against law enforcement databases containing "lookout" records from many agencies and the Terrorist Screening Database (TSDB) to identify travelers who are a threat to national security and should not be allowed to travel, and target travelers who need additional inspection upon arrival at a POE. The APIS system includes additional message processing audit capabilities that allow APIS Account Managers to see additional information related to the processing of each Manifest Message. The consolidated Advance Traveler Information user interface provides CBP users access to air, vessel, rail and bus manifest information via a single interface. It also enables PAUs to assess national security risks and prevent terrorists and other potential threats from entering the United States. In doing so, visibility into the manifest data, traveler watch list statuses, and results of queries on the manifest is provided.			
Key Facts			
Customer Transactions	5,200 Flights/Day 300K Cruise Passengers/Day 1.4 M Commercial Air Travelers/Day	**Data**	Oracle - 18 TBs
Primary Stakeholders	APIS Account Mangers, Passenger Analysis Units (PAU) at ports of entry (POEs), and secondary Customs and Border Protection (CBP) Officers. Passenger Manifests are submitted to APIS by airlines, private aviators, cruise lines, and bus and rail carriers.	**Current Hosted Environment**	NDC
Major Interfaces	Terrorist Screening Database (TSDB), INTERPOL for lost/stolen passport records	**Application Age**	Approx. 2 years since last modernization
Amplifying Business Information			
• APIS runs 280/300 million TECS/non-TECS queries/month for transactions. • APIS supports BEMA, APC, ELMA, GE, MPC, SAMN, and TPAC applications. • APIS shares 2 million rows of data with internal/external users daily.			
Key Technologies			
Presentation Layer	Application Type - Web App; JSF	**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Java 1.6; Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Requires PIV
Data Layer	MyBATIS; Data Types: Char; JSON; CLOB; BLOB	**Other**	IBM MQ

Arrival and Departure Information System (ADIS)

Arrival and Departure Information System (ADIS) – Interface and Support Processes Division			
The Arrival and Departure Information System (ADIS) is a data aggregation system that contains the travel history and immigration status for over 346 million unique individuals. The system determines if a foreign national traveler is in compliance with terms of their admission by matching arrival, departure and status update records. For travelers who overstay their Admit Until Date, ADIS calculates unconfirmed (in-country) and confirmed (out-of-country) overstays. As a biographic foundation system for Entry/Exit, ADIS primarily supports the missions of Entry/Exit reconciliation and admissibility associated with visa/non-visa overstays. ADIS determines whether the traveler is in Legal Status (LS), Adjustment of Status (AOS), a Confirmed Overstay (CO) or Unconfirmed Overstay (UCO). This status plays a key role in future admissibility decisions made by the Department of State consular officers abroad, and CBP officers at the ports of entry. ADIS is a data aggregation system that matches arrivals, departures, and status updates to unique persons to compile a complete travel history. ADIS has interfaces with 14 different systems. The graphic below shows ADIS in the middle, and the source systems that provide data to ADIS in orange on the left. Messages from TECS, the Automated Biometric Identification System (IDENT), Computer Linked Application Information Management System (CLAIMS3), Person Centric Query Service (PCQS), and the Student and Exchange Visitor Information System (SEVIS) flow into ADIS and are matched to existing identities in the system. If no identity exists in ADIS, a new identity is created.			
Key Facts			
Customer **Transactions**	3200 Web Application Users 3.6 million daily transactions 364+M identities	**Data**	Oracle 16 TBs, Annual growth: 1TB, Annual growth starting FY20: 2 TBs
Primary **Stakeholders**	CBP Officers and overstay analysts, USCIS Service Center analysts, ICE Agents and overstay analysts, ICE Student Visa admin, TSA Alien Flight School Program, Selected INTEL Community, USDOD	**Current** **Hosting** **Environment**	NDC
Major **Interfaces**	10 million TECS I-94 transactions/month; ADIS connectivity with CBP Automated Targeting System (ATS) supports identification of priority overstays for ICE	**Application** **Age**	Approx. 16 Years
Amplifying Business Information			
• ADIS is frequently used at CBP Secondary to research admissibility • ADIS connectivity with CBP's Automated Targeting System (ATS) supports vetting and identifying all National Security and Public Safety and other Priority Overstays to ICE for action • 3.9 billion events (arrivals, departures, immigration updates) • 7.2 billion observations stored • OFO expects near real time performance.			
Key Technologies			
Presentation **Layer**	Application Type - Web App; AngularJS; JSP; Spring MVC	**Backend** **Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Database Scripts; Deployment

Arrival and Departure Information System (ADIS) – Interface and Support Processes Division			
			Artifacts – C++ binaries and scripts
OS Layer	Red Hat Linux Enterprise 6.x/7.x	**IDE**	Eclipse for Java and C++
Middleware	WebLogic 12.x, IBM MQ 8, Kafka 2.11	**Security Layer/ Authentication**	Authentication Requires SSO; Requires PIV; Authentication - TECS CAS; Authentication Requires AD
Data Layer	Data Type - Char; Hibernate; JDBC; Data Type - Binary; CLOB; BLOB	**Other**	

Audit Screen Rendering (ASR)

Audit Screen Rendering (ASR) –Interfaces and Support Processes Division			
ASR is used primarily by OPR (Office of Professional Responsibility) as it logs the activity and specific screens used by officers.			
Key Facts			
Customer Transactions	Approx. 50 users	**Data**	Oracle 79 TBs, Growth approx. 3 TB/month
Primary Stakeholders	Office of Professional Responsibility	**Current Hosting Environment**	NDC
Major Interfaces	Lookout Records, NCIC, TDED, Incident Logs, CSIS, User Profile, CMIR	**Application Age**	4 years
Amplifying Business Information			
ASR provides information for OPR on what CBP staff has been doing.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS / ICAM OUD; Authentication uses AD for SSO
Data Layer	MyBATIS; Hibernate Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

Automated Passport Control (APC

Automated Passport Control (APC) – Inspection Processes Division

Automated Passport Control (APC) Service is designed to help travelers move more quickly through the U.S. border clearance process by entering information at a self-service kiosk. APC is a free service; use is voluntary. APC does not require pre-registration or membership.

The APC self-serve kiosks allow passengers to submit their customs declaration and biographic/biometric information electronically. The collected data is vetted via federal enforcement systems; a referral is returned and a receipt is issued. Travelers then present their passport, travel information and receipt to a Customs and Border Protection (CBP) officer for verification.

APC maintains the highest levels of protection when it comes to the handling of personal data or information. By removing the need for an officer to scan or manually input travel document data, CBP Officers are able to process travelers in about half the time. This process has resulted in a 20 to 40 percent decrease in wait times where APC is available.

APC provides the following benefits to the traveling public:

- Bypass the traditional passport control line
- Travel handles submission of biometric and biographic data, thus reducing wait times
- Expedited exit process
- Conveniently located at international ports in and around the United States and at international pre-clearance sites
- Allows international travelers to enter the U.S. with a minimal customs and immigration questioning
- No fees or pre-registration.

Key Facts

Customer Transactions	3200 Web Application Users 3.6 million daily transactions 364+M identities	**Data**	Oracle; 31.6 TBs
Primary Stakeholders	US and Canadian Citizens in Class B1 or B2, VISA Waiver with ETSA Approval (Class WB or WT), US Residents with Class C1 or C2, Non-immigrant or Border Crossing Classification of Admission	**Current Hosting Environment**	NDC
Major Interfaces	Manifest, IDENT, PQS, PXSE, PIP, TDED, ESTA	**Application Age**	Established 2014 (approx.. 4 years)

Amplifying Business Information

APC is a backend service supporting certified vendor kiosks.

Performance Monitoring Parameters:

* The following functions are monitored: Login count, APC Requests, IDENT (pre bio query, Verify 4), PQS Vetting, PXSE Vetting, PIP NCIC/NNSV Vetting, TDED Query, ESTA Vetting, PIP Encounter/I94 Query.

Key Technologies

Presentation Layer	.NET/ASP	**Backend Components**	Deployment Artifacts - WAR Files; Standalone JAR files; Database Scripts

Automated Passport Control (APC) – Inspection Processes Division			
OS Layer	Linux; Red Hat Linux Enterprise	**IDE**	.NET/C+; Java; Java 1.6; Python; Eclipse; Visual Studio
Middleware	DataPower; WebLogic	**Security Layer/ Authentication**	Authentication Requires SSO
Data Layer	MyBATIS; Spring; Data Type - Char; JSON; CLOB; Other	**Other**	

CBP Vetting (CBPV)

CBP Vetting (CBPV) – Interfaces and Support Processes Division			
The Customs and Border Protection Vetting (CBPV) system is a CBP Web-internet application with 24/7 availability. The system is accessible from anyplace, at any time, with any hand held and mobile devices that has a functional web browser. There is no need for any additional VPN, firewall, and security tokens. CBP Vetting offers users the ability to submit vetting requests via on-screen entry or by uploading vetting requested files that have conformed to specific formatting requirements. The application also offers the ability to view or download the vetted response file that is created as a result of the vetting request submission.			
Key Facts			
Customer Transactions	4,500,000 requests conducted in August 2018 2,400,000 responses conducted in August 2018 Allows multiple queries (no limit) to be submitted in a single request	**Data**	Oracle 100 GBs Growth: 40% / year
Primary Stakeholders	CBP Border Patrol, CBP Office of Field Operations, Department of State, Department of Labor, Immigration and Customs Enforcement, Citizenship and Immigration Services, U.S. Coast Guard, FBI Office of Intelligence and Investigative Liaison, Office of Operations and Coordination, Customs and Border Protection Airport Security Seal Program	**Current Hosting Environment**	NDC
Major Interfaces	TECS, Seized Assets and Cases Tracking System (SEACATS), Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC), FBI Interstate Identification Index (III), National Law Enforcement Telecommunications System (Nlets), Interpol data for review by other government agencies. CBP vetting is a User Interface and does not have any direct interfaces with any external entities. The back-end Contractor interface are TSSV and TECS Portal.	**Application Age**	10+ years; Pilot at 9 border crossings
Amplifying Business Information			
CBP Vetting's high-level business objectives align with CBP's and the Department of Homeland Security's (DHS) mission to be the guardian of our Nation's borders and core value of vigilance through the efficient processing of queries for TECS, SEACATS, FBI NCIC, FBI III, Nlets and Interpol databases.			
Key Technologies			
Presentation Layer	Application Type - Web App; JSP; Servlets; Struts 1	**Backend Components**	Deployment Artifacts - WAR Files

CBP Vetting (CBPV) – Interfaces and Support Processes Division			
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - Other
Data Layer	Spring; Data Type - Char; Data Type - BLOB	**Other**	

Combined Automated Operations System Land (CAOS)

CAOS – Inspection Processes Division			
Combined Automated Operations System Land (CAOS) is an application that allows port managers at land border ports of entry to: • Schedule, run, record, and report on enforcement operations by random computer selection or manual choice of operation and time • Move Officers from one primary lane to another in an unpredictable manner • Schedule random enforcement operations such as K9-search, trunk search, and 10-minute blitz operations randomly during a shift • Aim to disrupt spotters and prevent predictability of enforcement operations • Schedule random operations for Vehicle and Pedestrian Primary lanes			
Key Facts			
Customer Transactions	4,835 active users, 173 CAOS sites	**Data**	Oracle, Lane schedules and assignments for CBPO
Primary Stakeholders	CBPO Supervisors, CBPO	**Current Hosting Environment**	NDC
Major Interfaces	TECS	**Application Age**	Approximate 10 years old
Amplifying Business Information			
Key Technologies			
Presentation Layer	Java 1.8, HTML5, JavaScript, Swing	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse
Middleware	WebLogic, WebSphere MQ	**Security Layer/ Authentication**	Authentication - Other
Data Layer	Data Type - Char; Other	**Other**	

Consolidated Secondary Inspection System (CSIS)

Consolidated Secondary Inspection System (CSIS) – Interfaces and Support Processes Division
The Consolidated Secondary Inspection System (CSIS) is the Customs and Border Protection (CBP) system for recording results of Secondary Inspections. The system allows recording of data from various sources to provide a single view of additional research done on travelers wishing to enter the United States. This can be additional Admissibility checks beyond what is checked and verified at the Primary U.S. entry point, and/or in-depth checks of baggage and agriculture items.

Key Facts

Customer Transactions	17,000+ travelers arriving by Air or Sea are referred daily for additional inspections 21,000+ travelers arriving by Land are referred daily for additional inspections	**Data**	Oracle 16 TBs Approx. 30% annual growth
Primary Stakeholders	Field Operations Offices and Agriculture Specialists, CBP and OFO to research admissibility of goods	**Current Hosting Environment**	NDC
Major Interfaces	Primary Query results, Person Lookout data, Watchlist data, traveler document information, crossing history and more.	**Application Age**	9 Years

Amplifying Business Information

CSIS is “single stop shopping” for recording Secondary Inspections As the tool for recording results of Secondary Inspections, CSIS also supports the mission of admissibility of travelers or their possessions by providing links to a number of other systems which provide additional traveler information and history. CSIS provides a single point of access regardless of the environment or function. Access to information from other sources (e.g. Primary, Office of Biometric Identity Management (OBIM)) is also available.

Performance Monitoring Parameters:

Function	Objective	Threshold	Below Threshold
Login	<3 secs	3-5 secs	>5 secs
Enc-List Query	<3 secs	3-5 secs	>5 secs
Photo Query	<3 secs	3-5 secs	>5 secs
Save Bag Inspection	<3 secs	3-5 secs	>5 secs
Save Adm Inspection	<3 secs	3-5 secs	>5 secs
Save Agric Inspection	<3 secs	3-5 secs	>5 secs
Create New Encounter	<3 secs	3-5 secs	>5 secs
Get Hit List	<= 10 sec	11-30 secs	>30 secs
PIP NCIC	<3 secs	3-5 secs	>5 secs

Key Technologies

Presentation Layer	Application Type - Web App; HTML5/JavaScript; JSF; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files; Standalone JAR files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse

Consolidated Secondary Inspection System (CSIS) – Interfaces and Support Processes Division			
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires AD
Data Layer	Hibernate; JDBC; Data Type - Char; CLOB; BLOB; Other	**Other**	

Decal and Transponder Online Procurement System (DTOPS)

Decal and Transponder Online Procurement System (DTOPS) – I-Solutions Division			
The Decal and Transponder Online Procurement System (DTOPS) is a public facing Web-based online procurement system where commercial vehicle, private aircraft, and private vessel owners pay a yearly fee, rather than a per transaction charge, to cross the U.S. border by purchasing yearly user fee decals and transponders. DTOPS also supports an intranet site for Customs and Border Protection (CBP) access to accounts. DTOPS pushes the zone of security outward and advances the department and agency goals of securing the U.S. borders. The DTOPS website allows travelers to purchase decals and transponders for their vehicles in advance of travel which greatly reduces their wait time at the border. Through the DTOPS website, CBP Officers can enter paper applications, perform help desk and administration functions, and include a query capability for field users.			
Key Facts			
Customer Transactions	120,844 Transponder (Annual) orders were placed 156,306 Single Crossing orders were placed There are currently 299,517 active DTOPS accounts	**Data**	73 GB
Primary Stakeholders	BP Officers and members of the general public who need to purchase decals and transponders for their commercial and private vehicles.	**Current Hosting Environment**	CBP AWS Cloud East (CACE)
Major Interfaces	Pay.gov, Automated Commercial Environment (ACE) and Free and Secure Trade (FAST), SAP Financial Systems (SAP) is responsible for payment reconciliation with DTOPS. SAP interfaces with Pay.gov to ensure DTOPS payments are reconciled and notify DTOPS if payment issues occur.	**Application Age**	2 years - website redesign in FY16
Amplifying Business Information			
• In FY18–$52,527,135.00 was paid in vehicle, aircraft and vessel fees • December was the busiest month in 2017, processed approximately over 66,000 single crossings and transponders; collected $22,996,381.99 in fees.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSP; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.6; JavaScript; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV

Decal and Transponder Online Procurement System (DTOPS) – I-Solutions Division			
Data Layer	Hibernate; Spring; Data Type - JSON	**Other**	

Electronic Advance Passenger Information System (eAPIS)

Electronic Advance Passenger Info System (eAPIS) – Inspection Processes Division			
The Electronic Advance Passenger Information System (eAPIS) is a public-facing web-based interface, which allows small commercial carriers and private aviation operators to submit their flight manifests to CBP. eAPIS also provides viewing of Electronic System for Travel Authorization (ESTA) and Electronic Visa Update System (EVUS) results for authorized commercial carriers, administrative functionality for Customs and Border Protection (CBP) Office of Field Operations (OFO) account managers, and a web service Application Program Interface (API) for authorized commercial and private aviator users and organizations. eAPIS is the only channel for delivery of private aviation manifests into APIS/Manifest system for processing. eAPIS is a user-friendly, reliable method for submitting manifest data directly to CBP and receiving confirmation via e-mail of these transmissions. Upon completion of each transmission, a unique confirmation number is issued to the e-mail address provided during enrollment. The confirmation number provided to this email address can be used to track manifests. Mostly web services by general aviation and bus carriers. Some commercial airlines for crew processing			
Key Facts			
Customer Transactions	2,500 daily manifest submissions 10,000+ small commercial carriers use eAPIS 100,000 private aviators use eAPIS	**Data**	Same as APIS
Primary Stakeholders	Small commercial airline users, Private plane operators, Private plane owners, APIS national account managers (OFO), General public	**Current Hosting Environment**	NDC
Major Interfaces	APIS	**Application Age**	10 Years
Amplifying Business Information			
Key Technologies			
Presentation Layer	Application Type - Web App; JSP; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	WebLogic; WebSphere MQ	**Security Layer/ Authentication**	Authentication - Other
Data Layer	JDBC; MyBATIS; Data Type - Binary; Char Oracle db (stores session data, account info)	**Other**	IBM MQ

Electronic Secured Adjudication Forms Environment (eSafe)

Electronic Secured Adjudication Forms Environment (eSafe)– I Solutions Division			
The Electronic Secured Adjudication Forms Environment (e-SAFE), a new CBP web-based application built on the Salesforce platform will serve as the primary public-facing, interface for applicants to submit waiver applications directly to the Admissibility Review Office (ARO). Salesforce is a Cloud-based Software-as-a-Service (SaaS) customer relationship management (CRM) product that will be implemented relatively quickly as a layer on top of the current ARO module, allowing for online submission of forms, increased workflow management options, improved form standardization and automation, and streamlined communication with applicants. Improving office efficiencies, communication, and eliminating paper from the current process will significantly strengthen ARO's mission focus. With improved data quality and security, as well as fewer administrative duties, adjudicators can focus more effort and energy on vetting applicants and preventing dangerous aliens from entering the United States. In addition to cost savings and the ability to repurpose people to mission-oriented work, modernizing the I-212 and I-192 process will result in significant qualitative benefits for the alien, POEs, and for ARO, in both efficiency and accuracy. The Salesforce Implementation, Integration, and Support Services (SIISS) Blanket Purchase Agreement (BPA) is a multiple-award, government wide BPA that consolidates the government's Salesforce technical development, operations and maintenance, and implementation strategy requirements into one procurement vehicle that can replace numerous agency-specific contracts, reducing both contract duplication and the government's administration costs. The e-SAFE web application will replace the current manual submission process, which is a paper form.			
Key Facts			
Customer Transactions	New application not in production	**Data**	New application not in production
Primary Stakeholders	Point of Entry (POE) Officers ARO Officers to Adjudicate Waivers	**Current Hosting Environment**	Salesforce CRM SaaS offering; New application not in production
Major Interfaces	Pay.gov, Trillium	**Application Age**	New
Amplifying Business Information			
The e-SAFE will allow the ARO to adjudicate the request, and decide whether to issue a waiver to an inadmissible alien in a much shorter timeframe than today. A waiver by the ARO subsequently allows the alien the ability to apply for admission to the United States.			
Key Technologies			
Presentation Layer	Salesforce proprietary	**Backend Components**	Salesforce proprietary
OS Layer	Salesforce proprietary	**IDE**	Salesforce proprietary
Middleware	Salesforce proprietary	**Security Layer/ Authentication**	Salesforce proprietary
Data Layer	Salesforce proprietary	**Other**	Salesforce CRM SaaS offering

Electronic System for Travel Authorization (ESTA)

Electronic System for Travel Authorization (ESTA) – I-Solutions Division
The Electronic System for Travel Authorization (ESTA) is a web based system intended to enhance aviation security and strengthen the Visa Waiver Program (VWP) by screening potential travelers, determine their eligibility, and provide an authorization to travel to the United States in advance of travel. U.S. legislation required the Department of Homeland Security (DHS) to implement an electronic travel authorization system and other measures to enhance the security of the VWP. ESTA adds a layer of security that allows DHS to determine, in advance of travel, whether an individual is eligible to travel to the United States under the VWP and whether such travel poses a law enforcement or security risk. All nationals or citizens of VWP countries who plan to travel to the U.S. for temporary business or pleasure for 90 days or less under the VWP (INA § 217) will need authorization via ESTA to travel to the U.S. The ESTA goals are to: • Provide a user friendly, mobile accessible website for travelers to apply for their travel authorization in 23 different languages • Collect and assess information about VWP traveler in advance of travel • Provide additional information to Customs and Border Protection (CBP) Officers conducting inspections • Reduce delays associated with vetting at the ports of entry (POEs) • Reduce the number of travelers that are not admissible at the border Benefits for DHS: • Facilitates legitimate travel while enhancing the security of the VWP Benefits for CBP Officers: • Reduces border traffic and provides them with additional information on incoming travelers Benefits for Travelers: • Determines eligibility pre-travel and increases travel security • Good for two years and multiple trips • No visit to consulate – apply online Benefits for Carriers: • Facilitated the removal of the I-94W upon capability to interactively receive and validate ESTA status • Addresses concerns pre-travel and lessens the cost burdens involved with traveler inadmissibility

Key Facts			
Customer Transactions	2,000,000 txns daily	**Data**	2.7 TBs
Primary Stakeholders	CBP Officers Travelers in general public from VWP countries Carriers IC partners	**Current Hosting Environment**	NDC
Major Interfaces	APIS Pay.Gov TSSV Lookout Records ATS-P Primary and Secondary applications	**Application Age**	Approx. 10 years, 3 years since last modernization.

Electronic System for Travel Authorization (ESTA) – I-Solutions Division			
Amplifying Business Information			
• The website can also be accessed in 23 different languages, is user friendly, and can be easily accessed on mobile devices. • ESTA collected $211,966,884 in fees in Fiscal Year 2018 (FY18) • ESTA begun collecting social media information since December 2016 from applicants in order to enhance the vetting process • ESTA is targeted to migrate to the CBP AWS Cloud East (CACE) and upgrade its technology stack in FY19 ESTA response time objective: < 3 secs ESTA response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Application Type - Web App; Spring Web Flow, JSP	**Backend Components**	Deployment Artifacts - WAR Files, Standalone JAR files; Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse SQL Developer
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV
Data Layer	Hibernate; Spring; Data Type – JSON Data Type – XML Data Type – Char	**Other**	

Electronic Visa Update System (EVUS)

Electronic Visa Update System (EVUS) – I-Solutions Division
The Electronic Visa Update System (EVUS) is a web-based system that facilitates periodic updates of biographic information by U.S. visa holders from countries subject to EVUS requirements as mandated by the National Security Council and the Department of Homeland Security (DHS). EVUS determines eligibility of visitors with a 10-year B1 (business), B2 (tourism), and B1/B2 (Business/Tourism) visa to travel to the United States by checking against selected law enforcement databases to determine whether such travel poses a law enforcement or security risk. In alignment with the CBP mission "*To safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel*.", EVUS was developed as a way to obtain regularly updated biographic information from travelers to enhance the security of 10 year visa issuance. The EVUS goals are to: • Provide a user friendly, mobile accessible website for travelers to enroll in 2 languages • Collect and assess information about visitors with 10-year B1, B2, and B1/B2 U.S. visas in advance of travel • Provide additional information to Customs and Border Protection (CBP) Officers conducting inspections • Reduce delays associated with vetting at the ports of entry (POEs) • Reduce the number of travelers that are not admissible at the border Benefits for DHS: • Facilitates legitimate travel while enhancing the security of the 10-year visa issuance

Electronic Visa Update System (EVUS) – I-Solutions Division			
Benefits for CBP Officers: • Reduces border traffic and provides them with additional information on incoming travelers Benefits for Travelers: • Determines eligibility pre-travel and increases travel security • Good for two years and multiple trips Benefits for Carriers: • Facilitates interactive capability to receive and validate EVUS status • Addresses concerns pre-travel and lessens the cost burdens involved with traveler inadmissibility			
Key Facts			
Customer Transactions	EVUS processed 1,489,230 enrollments in Fiscal Year 2018	**Data**	268 GB
Primary Stakeholders	People Republic of China (PRC) as visitors or with a 10-year visitor Visa; CBP Officers Carriers IC partners	**Current Hosting Environment**	NDC
Major Interfaces	TDED APIS TSSV Lookout Records ATS-P Primary & Secondary applications	**Application Age**	2 years
Amplifying Business Information			
EVUS response time objective: < 3 secs EVUS response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Application Type - Web App; AngularJS	**Backend Components**	Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Atom, Visual Studio Community Edition (UI) Eclipse SQL Developer (DB)
Middleware	Application Type - Service App; Spring MVC, Tomcat	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV
Data Layer	JPA; Hibernate, Oracle Data Type - Char; Data Type – JSON Data Type – XML	**Other**	EVUS is targeted to migrate to the CBP AWS Cloud East (CACE) and upgrade its technology stack in FY19

Encounter Broker Services (EBS)

Encounter Broker Service (EBS) Interfaces Support Process Division			
The Encounter Broker Service (EBS) is a central gateway for DHS components to exchange terrorist watch list encounter nomination and resolution messages with the Terrorist Screening Center (TSC). The data centralization makes it possible for agencies to share encounter information with each other. EBS also provides Web user interface for users to create and submit encounter nomination and review. The EBS interface will include a standard request/response approach with EBS responding after the successful processing of a transaction or the submission of a reject with the reason for rejection. This will allow for better synchronization of data between sending and receiving systems. For system administration, the EBS will include capability to refresh or resend data to external partners and also configure/establish a new consumer for the EBS.			
Key Facts			
Customer Transactions	Encounter information transmitted between "Contractors" and TSC	**Data**	Oracle 10 GBs, Growth: 15 GB/year
Primary Stakeholders	DHS Office of Screening Coordination (SCO) ,CBP PSPD WL EBS Team, CBP , Targeting and Analysis Systems Program Directorate (TASPD) UPAX/TF Team, FBI's Terrorist Screening Center (TSC) , Contractors for Encounter data ,CBP – National Targeting Center (NTC) via CBP TASPD's UPAX/TF system ,Transportation Security Administration (TSA), TSA Secure Flight, TSA Credentialing, Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), US Coast Guard (USCG) US Secret Service (USSS)	**Current Hosting Environment**	NDC
Major Interfaces	Interfaces are as indicated in the "Primary Stakeholders" section	**Application Age**	2 years old
Amplifying Business Information			
EBS will allow DHS components to create and transmit pertinent data (terrorist identifiers) about Encountered Individuals (i.e. Encounter records) to TSC's Terrorist Screening System (TSS) in a real time fashion. DHS components will be able to create Encounter records via Passenger Services Program Directorate's (PSPD) Encounter user interface. In addition, EBS will also allow DHS Components to transmit Encounter data via a system to system interface.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; ReactJS	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO
Data Layer	MyBATIS; Spring; Data Type - JSON; Data Type - CLOB;	**Other**	

Enterprise Reporting (ER)

Enterprise Reporting (ER) – Interface Support Processes Division
Passenger Systems Program Directorate (PSPD) Enterprise Reporting (ER) provides a suite of reporting solutions that deliver improved reporting effectiveness using modern relational database systems, web services, and Business Objects Enterprise (BOE). ER is part of the TECS Modernization technical infrastructure tasked to modernize legacy TECS reports as well as centralize and standardize the reporting solutions within the Passenger Directorate. ER oversees the Integrated Advanced Passenger Information System (iAPIS). iAPIS, accommodates regulatory changes, integrates input resources, and automates many operational processes. iAPIS provides a more effective and comprehensive approach to identifying, ensuring, and enforcing Advance Passenger Information System (APIS) compliance as well as improved data integrity and retrieval. ER supports the Electronic System for Travel Authorization (ESTA) data marts that automate the creation and delivery of reports to improve and extend the reporting capability. The ESTA data mart solution provides a more effective and comprehensive approach to identifying, ensuring, and enforcing compliance for the ESTA program management office. ER maintains and generate reports from the Arrival and Departure Information System—Reporting (ADIS-R) which is a data warehouse application providing robust reporting and analytical capabilities based on ADIS data,. ADIS is an integral part of the solution for entry/exit transformation that combines biographic and bio-metric information in order to identify potential violations of immigration law, which assists officials with determining a foreign national's admissibility to the United States, eligibility for immigration benefits, or amenability to removal proceedings. ADIS-R provides users access to ADIS data for analysis and decision making. Users can benefit from a multitude of TECS modernized reports and various business functions located under Management Reporting on TECS Portal, which consolidates reports into one centralized area for ease of navigation. Empowers business users to create ad-hoc reports so they can respond to information requests quickly. Provides summarized metrics and charts for Arrivals and Departures by Locations and Admission Class, Dashboards for Key Performance Indicator metrics ER supports the Annual Overstay Report by providing data used by OFO to create overall and country-by-country statistics, a congressionally mandated report produced every January.

Key Facts			
Customer Transactions	• 176,942,000 records processed daily for iAPIS • 2,000,000 records processed daily for ESTA • 200,000 records processed yearly for ER Electronic Media • 1,716,267 records processed daily for ER PL/SQL • ADIS-R processes an average of 60 million records per day. This includes ADIS-R data loads and NCTC daily feeds.	**Data**	Oracle: ER – 0.25 TBs iAPIS - 1.4 TBs, Electronic Media - 5 GBs, ADIS-R – 20 TBs
Primary Stakeholders	Internal users within CBP at Office of Field Operations, Office of Information and Technology (OIT) Internal Revenue Service DHS Law Enforcement and the Intelligence Community	**Current Hosting Environment**	NDC
Major Interfaces	TECS, ADIS (via ADIS-R reports), ETSA, iAPIS from passenger manifests	**Application Age**	ER - 5 years; ADIS-R - 3 years

Enterprise Reporting (ER) – Interface Support Processes Division			
Amplifying Business Information			
• 213 total ER reports with 57 reports constituting 12 modernized business transactions deployed to TECS portal • 92 Standard ADIS-R Reports Deployed • iAPIS Reports available with previous days data for daily reports, previous months data for monthly reports • NCTC daily feed has a 1 day objective - Provides NCTC with data accumulated the very next day			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/CSS/JavaScript; JQuery 1.6.2; JSF; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files; Standalone JAR files; Database Scripts; Informatica Workflows; BusinessObjects Universes, Folders, Reports and Security
OS Layer	Linux – RH6.x	**IDE**	Java; JavaScript; Eclipse
Middleware	WebLogic; WebSphere MQ	**Security Layer/ Authentication**	Authentication - TECS CAS; Other; Requires SSO; Requires PIV
Data Layer	MyBATIS; Spring; Data Type - Char; JSON; CLOB; BLOB; Other	**Other**	Oracle Database; SAP BusinessObjects Reporting; Informatica PowerCenter for Extract, Transform and Load (ETL)

Flex Management Console (FMC) – Information Only

Flex Management Console – Land Border Integration Division			
LBI applications are outside of the scope of work defined in this document. A description of FMC is provided to illustrate where LBI applications interface with other PSPD applications. FMC interfaces with VPAIS for vehicular based information and indirectly LPAIS for traveler information. The Flex Management Console (FMC) is a LBI application designed and developed to allow users the ability to view the traffic transiting the Inbound, Outbound, Border Patrol, and Pedestrian environments in real-time. It is a Microsoft Windows thick-client application for CBP supervisors to monitor inspections at selected lanes by allowing them to view the biographic data, vehicle data, query results, and adjudication of all encounters. It also has a secondary functionality that allows users the ability to view and update Signage at selected air and lane POEs.			
Key Facts			
Customer Transactions		**Data**	N/A
Primary Stakeholders	• Office of Field Operations • Border Patrol • Land Border Integration	**Current Hosting Environment**	N/A
Major Interfaces	VPAIS/LPAIS	**Application Age**	6 years
Amplifying Business Information			
The FMC application allows CBP Supervisors and management to view traffic throughput at select lanes/sites to assist them with managing staffing needs. Its ability to view and update Signage lets Supervisors adjust			

Flex Management Console – Land Border Integration Division			
lane/site signage based on that throughput information. This helps the site operate more efficiently and reduces travel wait times. It also provides additional security for the inspecting Officer/Agent by letting others see backend queries that reveal potentially dangerous travelers.			
Key Technologies			
Presentation Layer	C#, .NET Framework	**Backend Components**	Internet Information Server
OS Layer	Windows Server; Windows 7/10	**IDE**	Visual Studio
Middleware	VPAIS/LPAIS	**Security Layer/ Authentication**	SSL/TLS 1.2, VPAIS/LPAIS/TECS login authentication/authorization
Data Layer	Microsoft SQL Server	**Other**	Git, SVN

Global Entry (GE) - Kiosks

Global Entry (GE) – Inspection Processes Division			
Global Entry (GE) provides pre-approved members of the traveling public automated, expedited processing through U.S. Customs by providing a self-service kiosk to complete their declaration into the United States. Global Entry eliminates the need for travelers to fill out forms and wait in line to be interviewed for admissibility and intent of their visit/return. GE provides a quick, biometric entry-exit screening system for low risk, pre-approved members.			
Key Facts			
Customer Transactions	40K transactions daily	**Data**	Oracle, 0.7 TBs
Primary Stakeholders	OFO, POEs, CBPOs, Global Entry members from: Columbia, United Kingdom, Germany, Netherlands, Panama, Singapore, South Korea, Mexico, Taiwan	**Current Hosting Environment**	NDC
Major Interfaces	GES; APIS Manifest; IDENT, PQS, APIS	**Application Age**	Approximately 10 years

Amplifying Business Information

7,537,015 trusted travelers with GE benefits (as of August 29,2018)

There are currently 829 GE Kiosks deployed in 74 airports.

GE enrolled it's 5 millionth member 2018

erformance Monitoring Parameters:

	Objective	Threshold	Below Threshold
System Exceptions	<10%	10% - 25%	>25%
Timeout	<10%	10% - 25%	>25%

* The following response times are monitored for trend analysis: total Session time, GES, PQS, NCIC, IDENT, and APIS Manifest queries.

Global Entry (GE) – Inspection Processes Division
GE kiosks are specialized equipment comprised of the following: LCD w/resistive touch screen, internal service keyboard w/trackball, standard thermal printer, Dell OptiPlex 5050 computer, signature keypads, phone and headset web camera. Specialized integration software is required to ensure all components operate in compliance with OIT operational and security standards and Mission Critical business functionality. GE kiosks are expected to be replaced with a facial recognition solution to identify GE members.

Key Technologies			
Presentation Layer	Application Type - Web App; Application Type - Thick Client; JQuery 1.6.2; Servlets; Struts 1; Swing	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	C/C++; Java; Python; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - Other
Data Layer	JDBC; Data Type - Char; JSON ;CLOB; Other	**Other**	

Global Entry - Facial Recognition (GE-Face)

Global Entry Facial Recognition (GE-Face) – Inspection Processes Division
The Global Entry program benefits CBP and participating foreign governments by allowing them to focus their efforts on unknown and potentially higher risk air travelers, thereby facilitating the movement of people in a more efficient and effective manner, while serving as a force multiplier for CBP. CBP is continuously working to improve the entry process for travelers and to realize the goal of increased security while expediting the flow of legitimate travelers. The benefit of Facial Recognition for Global Entry is the ability to handle higher volume processing faster than ever before. GE Facial uses the existing kiosks to collect a photo and accurately verify the identity of the GE member utilizing photo comparison from CBP holdings and provides facial matching along with backend vetting. The vision for Global Entry of the Future (GE Next Gen) is a kiosk-less solution that uses facial recognition to identify GE members.

Key Facts			
Customer Transactions	Currently 200-300 transactions/day at one POE. Additional POEs planned.	**Data**	See GE
Primary Stakeholders	See GE	**Current Hosting Environment**	See GE
Major Interfaces	GES; Manifest; backend vetting systems; TVS	**Application Age**	New capability; < 1 year.

Amplifying Business Information
GE-Face aligns with CBP's Biometric Entry-Exit strategy of identifying travelers with biometrics.

Global Entry Facial Recognition (GE-Face) – Inspection Processes Division			
Key Technologies			
Presentation Layer	See GE	**Backend Components**	See GE
OS Layer	See GE	**IDE**	See GE
Middleware	See GE	**Security Layer/ Authentication**	See GE
Data Layer	See GE	**Other**	

Global Enrollment System (GES)

Global Enrollment System (GES) – I-Solutions Division			
Global Enrollment System (GES) is the centralized system for managing enrollment into U.S. Customs and Border Protection's (CBP) Trusted Traveler, Registered Traveler, and Trusted Worker (TW) Programs. Trusted Traveler Programs (TTP) include NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), Global Entry (GE), and Free and Secure Trade (FAST). The TW programs include eBadge, Bonded Facility Vetting, and Broker's License. The systems manage centralized databases with global lookup and validation capability and standardize the business processes, business rules, and data for enrollment into these programs. **GES is the internal CBP tool used for processing applications, facilitating the risk assessment process, conducting interviews, and finalizing enrollments into these programs. GES interfaces with Targeting and Analysis Systems Program Directorate's (TASPD) Unified Passenger (UPAX) system for performing the U.S. biographic vetting for the Trusted Traveler Programs. For the Trusted Worker programs, GES has a Vetting Module which interfaces with the Treasury Enforcement Communication System (TECS) Screening Services to support the risk assessment process for those programs.** GES supports the enrollments in the Trusted Traveler Programs and the background check for the Trusted Worker Programs. GES enables CBP Enrollment Center (EC) Officers to capture fingerprints for the biometric check against the Office of Identity Management's (OBIM) Watchlist and the Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) database. The EC Officers can view the Risk Assessment Worksheet to determine the program eligibility.		
Key Facts			
Customer Transactions	Over 4 million GE members, Over 6 million trusted travelers with GE benefits, Over 40 million GE Kiosk transactions	**Data**	24 TBs - GES , 665 GBs - GESTW
Primary Stakeholders	CBP Officers and employees who support Trusted Traveler and Trusted Worker PROGRAMS.	**Current Hosting Environment**	NDC
Major Interfaces	TTP to receive application for SENTRI, NEXUS, Global Entry and FAST UPAX and TSSV for TW risk assessment Foreign governments for risk assessment GPO to produce TT cards TSA for TT PreCheck Produces photo galleries for TVS	**Application Age**	Version 4 is 13.3 years
Amplifying Business Information			

Global Enrollment System (GES) – I-Solutions Division
GES supports an electronic interface with more than 20 internal and external customers. GES contains more than 871,753 eBadge, 5,717 Broker License, and 10,584 approved Trusted Worker applicants. Global Entry members include 364,347 US Legal Permanent Residents and Foreign Country partner citizens. More than 3,758 CBP officers access GES from 140 enrollment centers or 49 enrollment on arrival airport (EoA) locations. Since July 2017, 64,495 travelers have been enrolled at one of the EoA locations GES response time objective: < 3 secs GES response time threshold: 3-5 secs Specialized Equipment supporting GES include Trusted Traveler Global Enrollment Center workstations and Trusted Traveler Mobile Enrollment Jump Kits. The Trusted Traveler Global Enrollment Centers enable CBP Officers to conduct interviews and finalize the Trusted Traveler application process. There are a total of 112 enrollment centers located across the country. The following equipment is used to support enrollment interviews and data capture to complete the GE application approval process: tower workstation, monitor, passport scanner, web camera, printer, signature pad, mouse, keyboard, and fingerprint scanner. Specialized integration software is required to ensure all components operate in compliance with OIT operational and security standards and mission critical business functionality. The Trusted Traveler Mobile Enrollment Jump-kits enables CBP Officers to conduct interviews and finalize the Trusted Traveler application process during special enrollment events and trade shows. There are a total of 100 mobile jump kits in circulation. The following equipment is used to support mobile enrollment interviews and data capture to complete the GE application approval process: laptop computer, passport scanner, web camera, printer, signature pad, mouse and fingerprint scanner stored in a mobile case for transportation. Specialized integration software is required to ensure all components operate in compliance with OIT operational and security standards and mission critical business functionality.

Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.8.3; JSP; Servlets; Struts 1	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; DataPower; WebLogic; WebSphere MQ	**Security Layer/ Authentication**	Authentication - Top Secret-LDAP; Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV
Data Layer	Hibernate; JDBC; JPA; Spring 2.5; Data Type - Binary; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB; Data Type - Other	**Other**	Oracle (DB)

I-736 Website

I-736 Website – I-Solutions Division			
The I-736 web is a public facing website that allows travelers from participating countries visiting Guam or Commonwealth of the Northern Marianas Island (CNMI) via air or sea to complete an I-736 Visa Waiver form. The ability to fill out the form electronically speeds up the processing at the arrival airport. Travelers can fill out the I-736 Visa Waiver form electronically prior to travel. Travelers can review and update their I-736 seven days prior to travel.			
Key Facts			
Customer Transactions	Since January 2018 over 205,000 unique website visitors	**Data**	none
Primary Stakeholders	Citizens of the following Countries: Australia, Brunei, Hong Kong, Japan, Malaysia, Nauru, New Zealand , Papua New Guinea, South Korea, Taiwan, Singapore, United Kingdom	**Current Hosting Environment**	CBP AWS Cloud East (CACE)
Major Interfaces	TDED	**Application Age**	<1 year
Amplifying Business Information			
Enhances security by capturing electronically the information supplied by Guam-CNMI visa waver travelers I-736 website launched in October 2017 Over 221,130 paper forms eliminated since January 2018			
Key Technologies			
Presentation Layer	Web App; AngularJS	**Backend Components**	Deployment Artifacts - WAR Files;
OS Layer	AWS Cloud	**IDE**	Eclipse
Middleware	Service App; Spring MVC, Tomcat	**Security Layer/ Authentication**	SSL
Data Layer	Data Type – JSON Data Type – XML	**Other**	

I-94 Website

I-94 Website – I-Solutions Division
The I-94 web is a public facing website that allows travelers who plan on entering the United States via a land border to apply for a provisional I-94. The ability to pay for and obtain a provisional I-94 prior to arriving at the Port of Entry speeds up the processing time for CBP officers and the traveling public. In addition, it supports the goal removing cash handling at the Port. In addition, travelers are able to retrieve their most recent I-94 and travel history. I-94 levies are paid via Pay.Gov Travelers: (1) entering US via land who wish to pay for I-94 prior to POE (2) who want copies of I-94 (3) view admission period (4) I-94 travel history.

Key Facts			
Customer	372,000 travelers paid in advance to get their	**Data**	None
I-94 Website – I-Solutions Division			
Transactions	provisional I-94 Over 62,000 provisional I-94s have been created since January 2018 24% of users access the I-94 website via handheld devices 76% of users access the I-94 website via desktop		
Primary Stakeholders	Travelers: (1) entering US via land who wish to pay for I-94 prior to POE (2) who want copies of I-94 (3) view admission period (4) I-94 travel history	**Current Hosting Environment**	CBP AWS Cloud East (CACE)
Major Interfaces	I-94 website coordinates with Travel Document and Encounter Data (TDED) to validate documents and store the traveler's provisional records, and TDED provides the most recent I-94. The I-94 website coordinates with the Arrival and Departure System (ADIS) to provide the traveler's most recent crossing history. ADIS can also provide a traveler's admission status. I-94 interfaces with Pay.gov to facilitate the payment for provisional I-94.	**Application Age**	5 years, updated 3 years ago
Amplifying Business Information			
ESTA check for validated Visa Waiver prior to purchase			
Key Technologies			
Presentation Layer	Web App; AngularJS	**Backend Components**	Deployment Artifacts - WAR Files;
OS Layer	AWS Cloud	**IDE**	Eclipse
Middleware	Service App; Spring MVC, Tomcat	**Security Layer/ Authentication**	SSL
Data Layer	Data Type – JSON Data Type – XML	**Other**	

Inspectional Operations Electronic Media (IOEM)

Inspectional Operations Electronic Media (IOEM) – Interface and Support Processes Division
Inspectional Operations Electronic Media **(**IOEM) is used for recording results of searching electronic media such as cell phones.

Key Facts			
Customer Transactions	Approx. 100/day	**Data**	Oracle 500 MBs, Approx. 25% annual growth
Primary	OFO Officers	**Current**	NDC

Inspectional Operations Electronic Media (IOEM) – Interface and Support Processes Division			
Stakeholders	USBP Agents OAM Agents	**Hosting Environment**	
Major Interfaces	CSIS	**Application Age**	3 years
Amplifying Business Information			
Supports CBP mission by providing formatted documentation of media searches.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JSF; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Standalone JAR files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS / ICAM OUD; Authentication uses AD for SSO
Data Layer	Hibernate; JDBC; Data Type - Char; Data Type - CLOB; Data Type - BLOB; Data Type - Other	**Other**	

Inspectional Operations Incident Log (IOIL)

Inspectional Operations Incident Log **(IOIL) – Interface and Support Processes Division**			
Inspectional Operations Incident Log (IOIL) is used to record out of the ordinary incidents that occur at the ports of entry.			
Key Facts			
Customer Transactions	Approx. 500/day	**Data**	Oracle 116 GBs, Growth 25% annually
Primary Stakeholders	OFO Secondary Officers	**Current Hosting Environment**	NDC
Major Interfaces	CSIS, SIGMA	**Application Age**	4 years
Amplifying Business Information			
Supports CBP mission by providing formatted documentation of incidents. Performance Monitoring Parameters:			

	Function	Objective	Threshold	Below Threshold	

Inspectional Operations Incident Log **(IOIL) – Interface and Support Processes Division**				
	Login	<3 secs	3-5 secs	>5 secs
	Get Incident	<3 secs	3-5 secs	>5 secs
	Search Incident	<3 secs	3-5 secs	>5 secs
	Get Image	<3 secs	3-5 secs	>5 secs
	Save Summary	<3 secs	3-5 secs	>5 secs
	Save Remarks	<3 secs	3-5 secs	>5 secs
	Submit for Approval	<3 secs	3-5 secs	>5 secs

Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS / ICAM OUD; Authentication uses AD for SSO
Data Layer	MyBATIS; Hibernate Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

Inspectional Operations Pre-Clearance Alerts (IOPC)

Inspectional Operations Pre-Clearance Alerts **(IOPC) – Inspections Processes Division**			
Inspectional Operations Pre-Clearance Alerts (IOPC) is used to notify incoming ports of entry of people who need to be evaluated for entry to the U.S.			
Key Facts			
Customer Transactions	Approx. 50/month	**Data**	Oracle, 1 GB Growth 25% annually
Primary Stakeholders	OFO Secondary Officers	**Current Hosting Environment**	NDC
Major Interfaces	N/A	**Application Age**	1 year
Amplifying Business Information			
Supports CBP mission by providing in-advance information to the POEs of possible non-desirables.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files

Inspectional Operations Pre-Clearance Alerts **(IOPC) – Inspections Processes Division**			
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS / ICAM OUD; Authentication uses AD for SSO
Data Layer	MyBATIS; Hibernate Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

LBI (Land Border Initiative) Mobile Client (LMC) – Information Only

Land Border Integration (LBI) Mobile Client (LMC) – Land Border Integration Division			
LBI applications are outside of the scope of work defined in this document. A description of LMC is provided to illustrate where LBI applications interface with other PSPD applications. LMC interfaces with VPAIS for vehicular based information and indirectly with LPAIS for traveler information. The Land Border Integration Mobile Client (LMC) is an application designed and developed for CBP Officers and Agents to monitor and process outbound vehicles, inbound pedestrians, and BP checkpoint traffic. It was specially designed to run on Microsoft Windows Panasonic M1/G1 tablet devices so that users can use it when "roaming" and not be attached to a booth workstation. The application when run on supported hardware can read travel documents and vehicle license plates for use in backend security queries. Its ability to use Wi-Fi and commercial cellular broadband networks allow users to process travelers anywhere there is a signal. The application also allows users to subscribe to selected lanes to view and monitor traffic being processed.			
Key Facts			
Customer Transactions		**Data**	
Primary Stakeholders	Office of Field Operations Border Patrol Land Border Integration	**Current Hosting Environment**	Client Software
Major Interfaces		**Application Age**	3 years
Amplifying Business Information			
The LMC application in conjunction with supported hardware allows CBP Officers and Agents to process vehicles and travelers outside the traditional POE and checkpoint inspections arena. Its standalone nature means Officers and Agents are able to take the inspection process to outbound and other areas without CBP workstation access without losing the ability to query traveler's biographic and vehicle data. It enhances CBP's ability to ensure travelers/vehicles entering and exiting the US are legitimate, while improving the security of Officers and Agents by providing them a means to run backend security queries. The monitoring capability provides additional security for processing Officers/Agents by allowing others to monitor their areas for potentially dangerous alerts.			
Key Technologies			
Presentation Layer	C#, .NET Framework	**Backend Components**	Internet Information Server

Land Border Integration (LBI) Mobile Client (LMC) – Land Border Integration Division			
OS Layer	Windows Server 2012R; Windows 7/8/10	**IDE**	Visual Studio
Middleware	VPAIS/LPAIS	**Security Layer/ Authentication**	SSL/TLS 1.2, VPAIS/LPAIS/TECS login authentication/authorization
Data Layer	Microsoft SQL Server 2016	**Other**	Git, SVN, Panasonic M1/G1 tablets, MRTD attachment

Land Border Web Reporting System (LBWRS)

Land Border Web Reporting System (LBWRS) – Inspection Processes Division
Land Border Web Reporting System (LBWRS) is an online series of reports and audit statistics, collected by the land border Primary Office of Information and Technology (OIT) that provide accurate and reliable statistical data on Pre-Primary and Primary lane functional operations at ports of entry (POEs) and Border Patrol checkpoints. LBWRS provides managers, directors, auditors, security, and operational personnel with accurate and reliable information on port activity that supports a multitude of reporting needs. LBWRS is just one of many resources utilized to fulfill our mission to secure our nation's borders while facilitating trade and travel. LBWRS is utilized by management to monitor and to help improve port and checkpoint, efficiency and accuracy. LBWRS also helps CBP ensure that the data received by the front line personnel is accurate and received as quickly as possible to assist with their traveler interviews. Reports and statistical data available: • Lane Status (LSS) is a supervisory tool that summarizes vehicle and lane activities. • Lane Status History (LSH) permits supervisors to view statistical detail of operational and hardware activity (at the inspection booth level) of vehicle traffic for a specific date. • ID Status History assists management in identifying and addressing Primary inspection processing anomalies. • Dedicated Commuter Lane (DCL) reports include: Persons Crossing Statistics, Authorized/Unauthorized Vehicles, Vehicle Inspection Times, Passenger Crossings per Day, Enrollee Inspection Times, Referral Status. • Other reports/data downloads/uploads include: Average Inspection Time, Average Response Time, OA (Operational Assessment) Report Download, End-to-End Response Time, Read Rates, Radio Frequency Identification (RFID) Read Count, Systems Response Time, and Lane Traffic, Department of State (DoS) RFID Usage, Specific State Enhanced Driver's License (EDL), Interpol Stolen and Lost Travel Documents (SLTD), Vehicle Package Count by License Plate, Vehicle Package searches and uploads, and Pre-Primary Lane equipment monitors.

Key Facts			
Customer Transactions	Reporting solution with 10,484 active users	**Data**	Vehicle and lane activities at Land Border crossing ports of entry. These activities include average response time, RFID and License Plate Reader read rates and RFID read counts
Primary Stakeholders	Office of Field Operations (OFO)	**Current Hosting Environment**	NDC

Land Border Web Reporting System (LBWRS) – Inspection Processes Division			
	Border Patrol HQ, Auditors, Port Directors, supervisory Border Patrol agents and Land Border Integration Division		
Major Interfaces	Vehicle Primary Activity Monitor (VPAM) Service TECS	**Application Age**	Approximately 9 years old
Amplifying Business Information			
Key Technologies			
Presentation Layer	Application Type - Web App; Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires PIV
Data Layer	EJB2; EJB3; Hibernate; JPA; Spring; Data Type - Binary; Data Type - Char; Data Type - BLOB	**Other**	

Lookout Records (LR)

Lookout Records (LR)– Interface and Support Processes Division			
Lookout Records (LR) is the Passenger Systems Program Directorate (PSPD)-centric system for all Lookout record types including Person, Vehicle, Organization, Aircraft, Vessel and Thing, DoS Consular Lookout & Support System (CLASS). These are provided to maintain support of services to internal and external agencies to create, update, and query functionality of shared LR. Lookout Records database, and service oriented system design provides increased accuracy and completeness of searches conducted against Lookout Records and other Lookout record centric data, integration with other systems, and increased flexibility to incorporate new capabilities for current and future needs to support the CBP mission.			
Key Facts			
Customer Transactions	250,000 requests daily; 5-10 million query requests per month responses conducted in September 2017 500,000 Lookout creation requests per month	**Data**	Oracle, 150 TBs
Primary Stakeholders	70,000 total users in 20 Federal agencies and contains data from CBP, USCIS, ICE, USSS, IRS, DEA, Treasury, Royal Canadian Mounted Police (RCMP), and the Intel Community	**Current Hosting Environment**	NDC
Major Interfaces	ICE CBP Targeting (TASPD) National Security Systems	**Application Age**	6 years old
Amplifying Business Information			

Lookout Records (LR)– Interface and Support Processes Division
Lookout Records is frequently used at CBP Secondary to research admissibility and provides information to multiple agencies and user communities on a daily basis. Office of Field Operations (OFO) is the #1 user of Lookout Records. Performance Monitoring Parameters:

Function	Objective	Threshold	Below Threshold
Login	<3 secs	3-5 secs	>5 secs
Create Person	<3 secs	3-5 secs	>5 secs
Create Vehicle	<3 secs	3-5 secs	>5 secs
Update Person	<3 secs	3-5 secs	>5 secs
Update Vehicle	<3 secs	3-5 secs	>5 secs
Delete Person	<3 secs	3-5 secs	>5 secs
Delete People	<3 secs	3-5 secs	>5 secs
Search Person UI	<3 secs	3-5 secs	>5 secs
Search Vehicle UI	<3 secs	3-5 secs	>5 secs
Search Person Service	<3 secs	3-5 secs	>5 secs
Search Vehicle Service	<3 secs	3-5 secs	>5 secs

Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; Eclipse; JDeveloper
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV; Authentication Requires AD
Data Layer	MyBATIS; Data Type - Binary; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB; Data Type - Other	**Other**	

Mitigation Adjustment Tool (M.A.T.)

Mitigation Adjustment Tool (M.A.T.) – Technical Integration Division
Mitigation Adjustment Tool (M.A.T) is a program used by system operators that provides a panel of buttons to execute scripts to display or update flags and configurations for PSPD Primary systems. The following applications can be adjusted based on the service degradation of IDENT and NCIC experienced at the time: TPAC, APC, GE, Pedestrian and US Arrival. This tool allows these application to continue and take normal course of processing of clients without waiting for real time responses. It allows an operator to enable/disable MINFST, ESTA, EVUS, TDED and PXSearch queries.

Mitigation Adjustment Tool (M.A.T.) – Technical Integration Division			
Key Facts			
Customer Transactions	N/A	**Data**	Not applicable
Primary Stakeholders	OFO, OIT/PSPD, BP	**Current Hosting Environment**	NDC
Major Interfaces	PSCNFG or REFLIB database tables	**Application Age**	March 2017
Amplifying Business Information			
Key Technologies			
Presentation Layer	Windows command line	**Backend Components**	Database scripts
OS Layer	Windows	**IDE**	Tcl scripting
Middleware	Not applicable	**Security Layer/ Authentication**	Windows AD authentication
Data Layer	Not applicable	**Other**	

Mobile Passport Control (MPC)

Mobile Passport Control (MPC) – Inspection Processes Division

Mobile Passport Processing (MPC) allows travelers to submit their Passport and Customs Declaration form via a smartphone instead of a traditional paper form. The Mobile Passport Control (MPC) app is free to download and use. The app is sponsored by the Airport Council International-North America (ACI-NA) and authorized by US Customs and Border Patrol.

MPC allows passengers to use their mobile devices to submit the customs declaration and biographic/biometric information electronically. The collected data is vetted via federal enforcement systems, and a referral is embedded in a Quick Response (QR) code written to the Traveler's device. Travelers then present their passport, travel information and QR receipt to a Customs and Border Protection (CBP) officer for verification.
Since the administrative tasks are performed by the traveler prior to the passport control inspection, MPC reduces passport control inspection time and overall wait times.

MPC is built on the backbone services of the Automated Passport Control (APC) system. MPC maintains the highest levels of protection when it comes to the handling of personal data, by removing the need for an officer to scan or manually input travel document data.

- MPC is a business transformation initiative in partnership with ACI-NA.
- ACI-NA and their technical partners have developed a mobile app that enables travelers to complete the customs declaration, submit passport information and upload a photo prior to inspection.
- MPC eliminates the need for interaction with the primary client, allowing more face to face interaction between the CBP Officer and the traveler, thus increasing the quality of inspections

Benefits to Travelers are:

- Bypass the traditional passport control line

Mobile Passport Control (MPC) – Inspection Processes Division			
• Offers the opportunity to create a profile for every member of the family • Traveler handles submission of biometric and biographic data, reducing wait times • Provides a more efficient in-person inspection between the CBP officer and the traveler • Expedited exit processing; traveler has access to faster lanes • Wi-Fi or cellular network is required to send information and receive a receipt but travelers may complete profile(s) without being connected • No fees or pre-registration required			
Key Facts			
Customer Transactions	313K transactions monthly	**Data**	Leverages APC database
Primary Stakeholders	United States Citizens Canadian Citizens traveling under Class of Admission B1 or B2	**Current Hosting Environment**	NDC
Major Interfaces	APC	**Application Age**	2 years
Amplifying Business Information			
Available at 24 US international airports and one sea POE			
Key Technologies			
Presentation Layer	.NET/ASP	**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Linux; Red Hat Linux Enterprise	**IDE**	.NET/C+; Java; Java 1.6; Python; Eclipse; Visual Studio
Middleware	DataPower; WebLogic	**Security Layer/ Authentication**	Authentication Requires SSO
Data Layer	MyBATIS; Spring; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - Other	**Other**	Includes .NET Client application for CBPO tablets/workstation.

NCIC/NLets Services (NNSV)

NCIC/NLTS Services (NNSV) – Interfaces and Support Processes Division
NNSV is the query service comprised of the National Crime and Information Center (NCIC)/The International Justice and Public Safety Network (Nlets), which provides Customs and Border Protection (CBP) with query / record entry access to the Federal Bureau of Investigation's (FBI) NCIC data and data owned by the states, Interpol, Immigration and Customs Enforcement (ICE), Canada, and the National Insurance Crime Bureau (NICB), via Nlets. NNSV also provides the service to override travelers who are repeatedly stopped by CBP because their name and date of birth are possible

NCIC/NLTS Services (NNSV) – Interfaces and Support Processes Division			
matches to an NCIC-wanted person list. NNSV provides both user interface and system to system services. The NNSV system provides one access point to both internal and external Passenger Systems Program Directorate (PSPD) consumers, and allows person and vehicle screening to be more easily combined with other services. NNSV supports CBP's mission of screening travelers entering the United States against FBI's NCIC, Nlets, and Canadian Nlets databases.			
Key Facts			
Customer Transactions	Approx. 2,000,000 transactions/day, across several functional areas.	**Data**	Oracle, 5 TBs, Growth: 5% a year
Primary Stakeholders	USDOJ, FBI, ICE, CBP , Canadian Nlets database	**Current Hosting Environment**	NDC
Major Interfaces	As listed in "primary stakeholders", Primary applications, Internal and external consumer interfaces.	**Application Age**	8 years
Amplifying Business Information			
One typical day, NNSV processes about 5 million person and vehicle queries for its consumers. NNSV response time objective: < 3 secs. NNSV response time threshold: 3-5 secs.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JSF; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO
Data Layer	MyBATIS; Spring; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

NCIC/NLets Services (NNSV) Revetting

NCIC/NLTS Services (NNSV) Revetting– Interfaces and Support Processes Division
The NCIC Recurrent Vetting (NNRevet) application is currently designed to receive enrolled Trusted Traveler participants from TASPD ATS UPAX (consumer). The NNRevet application was built to deliver vetting results to consumers in real time for subjects with record changes at NCIC. NNRevet system is designed and implemented as layered architecture, which is capable of receiving messages from different clients through different entry points represented in the Middleware or Web Services layer, further processing the message in the Service or Integration layer before sending messages to the services within CBP (NNSV, ASR, etc.) and beyond (NCIC).
Key Facts

NCIC/NLTS Services (NNSV) Revetting– Interfaces and Support Processes Division			
Customer Transactions	Varies according to business processes.	**Data**	Oracle, 1 TB Growth: 20%
Primary Stakeholders	Trusted Travelers	**Current Hosting Environment**	NDC
Major Interfaces	TASPD ATS UPAX	**Application Age**	5 years
Amplifying Business Information			
The Recurrent Vetting application has been designed to serve as a gateway for consumers to interface with NCIC customized re-vetting process. NNSV Revetting response time objective: < 3 secs. NNSV Revetting response time threshold: 3-5 secs.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JSF; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO
Data Layer	MyBATIS; Spring; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

Outlaying Area Reporting System (OARS)

Outlaying Area Reporting System (OARS – Inspection Processes Division
Note: OARS is being retired and travelers will use Reporting Outlying Area Mobile (ROAM) going forward. ROAM is outside the scope of this PWS. The Outlying Area Reporting System (OARS) was developed in the mid- to late-1990s to provide travelers entry into the United States at low-risk border entry points such as marinas, and recreation areas. The reporting units are self-contained climate-controlled rugged boxes, which house audio, video, and telephonic components. Each unit provides real-time audio and video capability via telephone lines that allow inspectors to communicate with travelers and see visual images of the traveler's face and travel documents (e.g., driver's license, passport, NEXUS card, etc.). Currently, there are 37 remote units in operation mostly around the northern Great Lakes region, from Minnesota to Maine. Boaters must report their arrival to U.S. Customs and Border Protection (CBP) if they have engaged in any of the activities below: • After they have been at any foreign port or place, including tying up at a foreign dock. • After having contact with any hovering vessel. The OARS program allows boaters that are not enrolled in the I-68 Program or NEXUS Program a way to present themselves for face-to-face inspection with a CBP officer at any of the OARS.

Outlaying Area Reporting System (OARS – Inspection Processes Division			
OARS satisfies 19 United States Code and 8 Code of Federal Regulations requirements for United States citizens, Lawful Permanent Residents of the United States, Canadian citizens, Landed Commonwealth Residents of Canada, and nationals of designated Visa Waiver Pilot Program countries with a valid, stamped I-94 or I-94W, Arrival/Departure to report their arrival into the U.S.			
Key Facts			
Customer Transactions	Not applicable – video phone system.	**Data**	Not applicable
Primary Stakeholders	U.S. Customs and Border Protection (CBP) inspectors a remote way of interviewing, checking, and logging travelers into the United States. OARS requires coordination and resources from the Office of Information Technology (OIT) and Office of Field Operations (OFO).	**Current Hosting Environment**	Not applicable.
Major Interfaces	None – OARS is a remote audio and video solution.	**Application Age**	20+ Years
Amplifying Business Information			
OARS is near end of life. OARS is being replaced by ROAM. Installation was completed on the original OARS system in Morristown Waddington, Ogdensburg, and Clayton, New York in July, 1997. OIT testing of remote and monitoring site videophone units is conducted on a daily basis M-F from the Passenger Systems Program Directorate (PSPD) facility in Columbia, MD. This test is conducted to provide reasonable confidence that the unit is operational and meets CBP's reporting requirements. The test also provides early warning of a problem to expedite the repair process.			
Key Technologies			
Presentation Layer	Not applicable	**Backend Components**	Not applicable
OS Layer	Not applicable	**IDE**	Not applicable
Middleware	Not applicable	**Security Layer/ Authentication**	Not applicable
Data Layer	Not applicable	**Other**	All OARS videophone unit are based on a microprocessor called the "8 by 8"

Payment Services

Payment Services – I=Solutions Division
Payment Services is a Web Service to CBP Internet applications with a need to collect a fee from public users through the interface with the Financial Management System's Pay.gov application. Payment Services provides the following functionality: • Provides payment collection screens in multiple languages to client applications. • Submits payment requests to Pay.gov for processing and returns payment processing results from Pay.gov back to CBP client application. • Provides a query mechanism for clients to determine payment results. • Provides a service to download the Pay.gov activity files for payment reconciliation.
Key Facts

Payment Services – I=Solutions Division			
Customer Transactions	Processed 27,833,822 client payment transactions with total amount of $460,367,427 in Fiscal Year 2018 (FY18)	**Data**	7 GB
Primary Stakeholders	Internal CBP internet applications that collect fees.	**Current Hosting Environment**	CBP AWS Cloud East (CACE)
Major Interfaces	Pay.gov ESTA TTP DTOPS I-94 website	**Application Age**	11 years
Amplifying Business Information			
Key Technologies			
Presentation Layer	N/A	**Backend Components**	Deployment Artifacts – Standalone Java Docker containers
OS Layer	Centos Linux, Docker container	**IDE**	Eclipse MySQL Workbench
Middleware	Application Type – Service App; Spring Boot, Tomcat	**Security Layer/ Authentication**	HTTPS/TLSv1.2
Data Layer	Spring Data Rest, JPA, Hibernate, MySQL Data Type – Char Data Type - XML	**Other**	

Pedestrian (PED Application

Pedestrian (PED) – Inspection Processes Division
Pedestrian Primary Processing (PED) was created in accordance with several Congressional mandates requiring the Department of Homeland Security to create an integrated, automated entry exit system that records and matches the arrivals and departures of aliens. The Pedestrian application is used as a tool for querying travelers crossing land borders on foot, on a bicycle, or in a bus. This application utilizes the TECS system to gather information and run queries based on the information given to the officer at the Primary workstation. It can also query: Global Enrollment System (GES), Enhanced Drivers' Licenses (EDL)/Enhanced Tribal Cards (ETC), and US Passports. The Pedestrian application allows the users to query various travel documents used at the border by foreign nationals in order to enhance national security and ensure the integrity of our immigration system. PED is deployed at all ports of entry (POEs) to allow for the verification of travelers entering into the United States on foot, by bicycle, or in a bus. Query data captured by: Machine Readable Zone (MRZ) cards • Manual entry via the keyboard • Radio Frequency Identification Document (RFID) reads Secure Electronic Network for Travelers Rapid Inspection (SENTRI) and NEXUS cards

Pedestrian (PED) – Inspection Processes Division

Queries: TECS Lookouts

- National Crime Information Center (NCIC)
- Interpol Stolen and Lost Travel Documents (SLTD) queries for foreign passports
- Compliance Measurement Examination for Passenger (COMPEX)
- Electronic Visa Update System (EVUS) and Student and Exchange Visitor Information System (SEVIS) queries
- I -94

Key Facts

Customer Transactions	Average 125,000 pedestrian a day	**Data**	Border crossing data for travelers crossed the border on foot
Primary Stakeholders	PED is used by Customs and Border Protection (CBP) port officers at a majority of the northern and southwest border ports of entry, and by multiple intelligence community agencies.	**Current Hosting Environment**	NDC
Major Interfaces	TECS Primary Query Service (PQS) Primary Inspection Process (PIP) Office of Biometric Identity (OBIM) GES	**Application Age**	Approximate 12 years old

Amplifying Business Information

Performance Monitoring Parameters:

Function	Objective	Threshold	Below Threshold
PIP Login	<3 secs	3-5 secs	>5 secs
PIP Person Query	<3 secs	3-5 secs	>5 secs
PIP NCIC	<3 secs	3-5 secs	>5 secs
PQS TECS Hit Query	<3 secs	3-5 secs	>5 secs
GES Doc	<3 secs	3-5 secs	>5 secs
EDL (enhanced driver's license)	<3 secs	3-5 secs	>5 secs
Land Passport Service	<3 secs	3-5 secs	>5 secs
PQS Admit	<3 secs	3-5 secs	>5 secs
IDENT: Verify 4	<20 secs	20-30 secs	>30 secs
IDENT: Identify 10	<20 secs	20-30 secs	>30 secs

Key Technologies

Presentation Layer	Application Type - Thick Client; Spring MVC; Swing	**Backend Components**	Deployment Artifacts - EAR Files

Pedestrian (PED) – Inspection Processes Division			
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.7; Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires PIV
Data Layer	EJB2; EJB3; Hibernate; JDBC; Spring; Data Type - Binary; Data Type - Char	**Other**	

Pleasure Boat Reporting System (PBRS)

Pleasure Boat Reporting System (PBRS) – Inspection Processes Division

The Pleasure Boat Reporting System (PBRS) collects, reports, and analyzes information related to the arrival of pleasure boats and associated travelers into the United States.

The PBRS stores arrival registration data in a central repository and its automated interfaces allow for immediate National Crime Information Center (NCIC) and TECS checks against enforcement and existing enrollment databases.

This information helps the flow of boating traffic and greatly improves targeting for potentially high-risk arrivals. In addition, the capability to collect and retrieve information produces data that can be analyzed and reported.

Through PBRS's related programs and subsystems, CBP Officers can access enforcement databases to maximize necessary actions. This enables CBP officers' consistent access and action to protect US borders.

PBRS provides these benefits:

- Record of traveler and boat identification information (specifically, for boats that enter the U.S. from foreign ports)
- Report of inspection results of pleasure boat arrivals (the arrival of a boat and its associated passengers)
- Verification of the identity of individuals enrolled in PBRS programs
- Analysis of travel data
- Small Vessel Reporting System (SVRS) registered enrollment data lookup
- New interface for Reporting Offsite Arrival-Mobile (ROAM) application to share or submit arrivals and inspections data

PBRS Program and Subsystems:

- The Local Boater Option (LBO) is a voluntary program that allows eligible small pleasure boat operators and passengers who are U.S. citizens (USCs) or Lawful Permanent Residents (LPRs) of the United States to enroll with CBP
- LBO enforcement checks are conducted through TECS queries and the information is stored in the TECS PBRS database
- Vessel Encounter (VE) is a sub-system of PBRS. VE records all enforcement stops made on vessels
- Cruise License (CL) is a sub-system of PBRS. CL records information on documented foreign yachts with a pleasure license endorsement entering the U.S. with the intent to cruise specified domestic waters.

Key Facts			
Customer Transactions	50,975 pleasure boat inspections in 2018 205,441 pleasure boat person arrivals in 2018 66,917 pleasure boats in 2018	**Data**	Oracle
Primary Stakeholders	Customs and Border Protection (CBP) Officers use PBRS to enforce the collection of user fees and maintain travel history	**Current Hosting Environment**	NDC

Pleasure Boat Reporting System (PBRS) – Inspection Processes Division			
Major Interfaces	NNSV, Lookout, PQS, and ROAM	**Application Age**	3 Years
Amplifying Business Information			
NOTE- SVRS is end of life. SVRS converted into PBRS registered boaters.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Servlets	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Unix	**IDE**	Java 1.6; JavaScript; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS
Data Layer	JDBC; MyBATIS; Data Type - CLOB	**Other**	

Portable Automated Lookout System (PALS)

Portable Automated Lookout System (PALS) – Inspection Processes Division			
The Portable Automated Lookout System (PALS) is a standalone application that assists U.S. Customs and Border Protection (CBP) officers in preventing the entry of illegal aliens, terrorists, and other individuals into the United States. PALS is used when online systems, such as TECS, are not available or at remote sites where there is no network connectivity available (e.g., small airports, private marinas, and onboard ships). PALS also helps determine if a vessel seeking access to a U.S. berth has had fines levied against it by the Fines, Penalties & Forfeitures Division (FPFD). • PALS is required as a part of the mitigation strategy to prevent the entry of illegal aliens, terrorists, and other individuals into the United States in cases where the CBP network is unavailable. • PALS is electronically installed on CBP workstations and laptops and the PALS DVD password is provided to OFO • OFO verifies the PALS password and applications are operational on Primary/Secondary workstations and laptops. PALS is portable and can operate on a local area network (LAN), stand-alone workstations, or laptops. PALS provides functionality similar to TECS; however, without the capability of modifying or adding records when there is no network connectivity. It allows users to specify and run queries on an extract of TECS and FPFD records.			
Key Facts			
Customer Transactions	PALS supports over 300 sites for offline operations.	**Data**	N/A
Primary Stakeholders	CBP Officers use PALS when other online systems are not available or at remote sites. PALS requires coordination and resources from the Office of Information Technology (OIT), Office of Field Operations (OFO), the Enterprise Data Management and Engineering Directorate (EDMED) and the Desktop Management Group (DMG)	**Current Hosting Environment**	N/A

Portable Automated Lookout System (PALS) – Inspection Processes Division			
Major Interfaces	TECS	**Application Age**	22 years

Amplifying Business Information

- PALS went operational in 1996 and is used at 300 sites
- PALS software is distributed electronically to workstations and laptops at Ports of Entry (POEs)
- An extract of TECS is copied to DVD's, encrypted/password protected, serialized, mailed and tracked to CBP POEs
- PALS is the Passenger System Program Directorate's only standalone application

PALS is targeted for retirement.

Key Technologies			
Presentation Layer	Application Type - Thick Client; Swing	**Backend Components**	Deployment Artifacts - EAR Files
OS Layer	Red Hat Linux Enterprise; Windows	**IDE**	Java 1.8; Eclipse
Middleware	WebLogic; N/A Middleware	**Security Layer/ Authentication**	Authentication - Other; Authentication Requires PIV
Data Layer	JDBC; Spring; Data Type - Binary; Char; JSON; CLOB; BLOB; Data Type - Other	**Other**	

Pre-Departure Service (PDS)

Pre-Departure Service (PDS) – I-Solutions Division

Pre-Departure Service (PDS) is a CBP internal application that works with TSA's Secure Flight (SF) program to obtain and deliver inbound passenger data. PDS works in tandem with SF and the DHS Router to deliver passenger screening results to an Airline Operator (AO). PDS provides participating airlines the ability to verify an international traveler's authorization to enter the U.S. thereby safeguarding America's borders and protecting the public from dangerous people. To determine each traveler's status, PDS analyzes which document checks are required (e.g. Passport check against ESTA for a Visa Waiver Program (VWP) traveler. PDS allows travelers to be vetted before they board the plane.

Key Facts			
Customer Transactions	PDS handles more than 66,000 requests per hour	**Data**	10 TBs
Primary Stakeholders	Airlines check international travelers coming into the United States. PDS checks for the following traveler's status: Electronic Visa Update Status (EVUS), Electronic System for Travel Authorization (ESTA), Document Validation, U.S. Passport check, VISA	**Current Hosting Environment**	NDC
Major Interfaces	EVUS ESTA TDED	**Application Age**	6 years

Pre-Departure Service (PDS) – I-Solutions Division			
	VISA		
Amplifying Business Information			
• Cruise lines will check travelers for valid ESTA • Green Card vetting • PDS operates 24/7 supporting international travelers. PDS has an overall objective of 2.5 seconds to return a response to DHSRouter who forwards it on to the airlines.			
Key Technologies			
Presentation Layer	None	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	SSL
Data Layer	Spring	**Other**	Internal application with no web interface.

Primary Inspection Process (PIP)

Primary Inspection Process (PIP) – Inspection Processes Division			
Primary Inspection Processes (PIP) is a modernized TECS system that supports primary processing. PIP is a single consolidated source for integration and shared services foundational to the CBP inspections processes. It allows person screening functions to be more easily combined with other services to support end-to-end inspection processes. PIP benefits its CBP users by providing fast and seamless access to critical information in support of admission and enforcement decisions. PIP sits between CBP's various consumer applications and the services they require in order to respond to evolving threats. PIP provides critical services to all primary applications in order to maintain the CBP Officer's ability to screen passengers entering the United States: • PIP provides alarms and alerts processes to notify primary and secondary of lookout information displayed at primary. • Provides consumer applications access to consolidated hit information (NCIC, TECS, etc.). • Provides consumer applications with access to travel document information. Provides consumer applications the ability to create/maintain I94/I94W records. • Provides CBP Officers with Secondary Inspection query information			
Key Facts			
Customer Transactions	A typical week within PIP will see over 1M encounters per day. Holidays will see increased volume. Traditionally, the busiest Land Border Day is Good Friday	**Data**	MsSQL – 4TBs
Primary Stakeholders	CBP Officers who utilize Primary applications for Land, Air and Sea.	**Current Hosting Environment**	NDC
Major Interfaces	Every primary applications (SA, US Arrival, TPAC, ACE, VPC, GE, APC/MPC, CAOS,),	**Application Age**	4 years (PIP modernized deployed in 2014)

Primary Inspection Process (PIP) – Inspection Processes Division			
	TDAD, CJIS, ADIS, CSIS		
Amplifying Business Information			
Zero downtime objective to support primary inspections PIP Queries response time objective: < 3 secs PIP Queries response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Not applicable	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.6; Java 1.8; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	
Data Layer		**Other**	IBM MQ

Primary Lookout Override (PLOR)

Primary Lookout Override (PLOR) – Interfaces and Support Processes Division			
Primary Lookout Override (PLOR) is an application that is used to override hits on travelers which are not actually against that specific traveler.			
Key Facts			
Customer Transactions	Approx. 5K/day	**Data**	Oracle 120 GBs Approx. 25% annual growth
Primary Stakeholders	OFO Secondary Officers	**Current Hosting Environment**	NDC
Major Interfaces	TASPD/UPAX, PSPD Primaries	**Application Age**	9 years
Amplifying Business Information			
Supports CBP mission by eliminating the need for sending travelers for additional exams when not needed.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JSF; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Standalone JAR files

Primary Lookout Override (PLOR) – Interfaces and Support Processes Division			
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS / ICAM OUD; Authentication uses AD for SSO
Data Layer	Hibernate; JDBC; Data Type - Char; Data Type - CLOB; Data Type - BLOB; Data Type - Other	**Other**	

Primary Query Service (PQS)

Primary Query Service (PQS) – Inspection Processes Division
Primary Query Service (PQS) provides CBP Officers with improved backend processing capabilities to perform person and conveyance searches. PQS integrates available data within TECS to improve the effectiveness and efficiency of primary inspections. PQS provides CBP Officers with TECS queries for vehicles and persons, as well as encounter and crossing history on travelers. PQS also provides various data-sharing capabilities with external agencies, international partners, and internal offices to provide a robust and seamless network of passenger information. PQS Benefits its users by providing fast and seamless access to TECS queries in order to provide traveler information to the CBP Officers. PQS provides critical functions to primary applications in order to maintain the CBP Officer's ability to screen passengers entering the United States PQS provides the following but is not limited to: • TECS Person Lookout Query • TECS Person Encounter Creation and History Query • TECS Vehicle Encounter Creation and History Query • TECS Vehicle Lookout Query

Key Facts			
Customer Transactions	Over 6,000,000 queries are requested and stored daily A typical day could create over 2,000,000 crossing records.	**Data**	Oracle Db with MsSQL stored procedures – 7 TBs
Primary Stakeholders	CBP Officers who utilize Primary applications for Land, Air and Sea will use PQS. Over 30 Consumer applications rely on PQS data for screening decisions to travel. External PSPD Consumers: ACE, I-94 Exit Mobile, vBEMA, ELMOp (Air-Sea and Land), OARS, TCN, TASPD Internal PSPD Consumers: APIS, PALS/TPAC Migration, PIP , SA (SAMN/SAPN), DCL, MOC, Land Primary Applications (6 Apps), PBRS, Kiosks APC/GE, Ready Lane, Manifest, CSIS (PLOR), TDED (IA21), PDS, TPAC International Consumers:	**Current Hosting Environment**	NDC

Primary Query Service (PQS) – Inspection Processes Division			
	CBSA (Send and Receive Data), Mexico RFID (Send and Receive Data)		
Major Interfaces	NICB TECS Portal (Alarm and E-Mail) Canadian Border Services Agency (CBSA) Mexico	**Application Age**	5 years (modernized PQS released in 2013)
Amplifying Business Information			
Zero downtime objective to support primary applications. PQS response time objective: < 3 secs PQS response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise; Unix	**IDE**	Java 1.8; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication Requires AD
Data Layer	Spring; Data Type - Char	**Other**	

Private Aircraft Enforcement System (PAES)

Private Aircraft Inspection Service (PAES) – Inspection Processes Division
The Private Aircraft Enforcement System (PAES) is a web-based system that gives Customs and Border Protection (CBP) officers the ability to process and access all inbound private aircraft arrival. Inbound flights are all flights with departure locations outside of the United States. Since November 2008, unscheduled commercial and private passenger flights arriving or departing the U.S. are required to submit Advance Passenger Information System (APIS) manifests using the Electronic Advance Passenger Information System (eAPIS) to CBP. This system was created to give the user the ability to inspect, process, and access all inbound private aircraft arrival. CBP officers can access queries the aircraft registration number or tail number and check the pending Aircraft Arrivals screen before the aircraft's arrival. PAES was established to: • Require all private aircraft to report to Customs for clearance one hour in advance of intended landing at an airport. • Channel all private aircraft, unless specially exempted, into the airport nearest the point at which the aircraft will cross the U.S. border or coastline. • FLIGHT PROCESSING - This interface allows authorized users to query and display grant or denial of flight landing rights via a user interface • MAINTAIN OVERFLIGHT EXEMPTIONS - This interface allows authorized users to add/update/query

Private Aircraft Inspection Service (PAES) – Inspection Processes Division			
overflight records and to copy over flight exemption data to another aircraft record • MANUAL FLIGHT ADDITIONS - This interface allows authorized users to submit a new manifest or add travelers to an existing manifest • TARP ADMINISTRATION - The Tactical Assessment of Radiation Procedures (TARP) is a new interface that allows authorized users to help ensure the full set of general aviation inspections processes are followed and practiced in accordance with the desired guidance			
Key Facts			
Customer Transactions		**Data**	
Primary Stakeholders	Customs and Border Protection (CBP) Officers use PAES to inspect, process, and access all inbound private aircraft arrival information	**Current Hosting Environment**	NDC
Major Interfaces	APIS	**Application Age**	3 Years
Amplifying Business Information			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Servlets	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Unix	**IDE**	Java 1.6; JavaScript; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication Requires SSO; Authentication Requires PIV
Data Layer	JDBC; MyBATIS; Data Type - CLOB	**Other**	Currently using IBM MQ. Plans to convert to web services layer

Protected Person Lookup Service (PPLS)

Protected Person Lookup Service (PPLS) – I-Solutions Division			
Protected Person Lookup Service (PPLS) is a web service that provides systems that have a need to share data outside of DHS and DOJ with the ability to match their data against the latest protected class list of visa types T (victims of human trafficking), U (victims of crimes) and VAWA (violence against women act petitioner) (T/U/VAWA) that is maintained by United States Citizenship and Immigration Services (USCIS) so proper protection can be placed on these records prior to sharing with agencies outside of DHS and DOJ.			
Key Facts			
Customer Transactions	Over 16M client requests processed in the last 5 months	**Data**	48 GB
Primary Stakeholders	Internal CBP applications that share data with IC partners	**Current Hosting Environment**	CBP AWS Cloud East (CACE)

Protected Person Lookup Service (PPLS) – I-Solutions Division			
Major Interfaces	USCIS ESTA EVUS	**Application Age**	Approx. 2 years
Amplifying Business Information			
Key Technologies			
Presentation Layer	N/A	**Backend Components**	Deployment Artifacts - Standalone Java Docker containers
OS Layer	Centos Linux, Docker container	**IDE**	Eclipse Cassandra Query Language Shell (cqlsh)
Middleware	Application Type - Service App; Spring Boot, Tomcat	**Security Layer/ Authentication**	HTTPS/TLSv1.2
Data Layer	Spring Data Rest, JPA, Spring Data Cassandra Data Type – Char, Data Type – XML Data Type - JSON	**Other**	

PSPD Application Response Time (PART)

PSPD Application Response Time (PART) – Technical Integration Division			
PSPD Application Response Time (PART) monitors transaction rates and response times for PSPD primary and secondary applications as per agreed upon threshold values before the system is affected.			
Key Facts			
Customer Transactions	Approx. 1.5 million MQ messages per hour	**Data**	P582 database which is shared among many different apps
Primary Stakeholders	OFO, OIT/PSPD, OBP	**Current Hosting Environment**	NDC
Major Interfaces	Monitors PSPD primary and secondary applications.	**Application Age**	7 years old
Amplifying Business Information			
Key Technologies			
Presentation Layer	Java web application (Servlets/JSPs) running on Windows servers with highly specialized SQL queries	**Backend Components**	WAR files on Windows, JARs and shell scripts on Linux

PSPD Application Response Time (PART) – Technical Integration Division			
OS Layer	Windows servers, Linux VMs	**IDE**	Eclipse IDE, NetBeans, Notepad++, Java 1.7, 1.8, ANT build environment
Middleware	Standalone Java services running MQ listeners, MQ messages for PART, JSON data format for TECS dashboard API	**Security Layer/ Authentication**	Oracle database authentication
Data Layer	Oracle 12.1 Enterprise (P582 PROD)	**Other**	v2.76, Application monitored are TPAC, APC, GE, PED, USARRIVAL, CSIS, LR, VPC

Registration Services

Registration Services –I-Solutions Division			
Registration Services is used solely by DTOPS to validate a user's login id and password.			
Key Facts			
Customer Transactions	120,844 Transponder (Annual) and 156,306 Single Crossing orders were placed by DTOPS users. Each time a DTOPS users logged into their account a transaction with Registration services would have occurred.	**Data**	43 GB
Primary Stakeholders	DTOPS end users	**Current Hosting Environment**	NDC
Major Interfaces	None	**Application Age**	7 years
Amplifying Business Information			
Supports DTOPS users.			
Key Technologies			
Presentation Layer	Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Linux	**IDE**	Java 1.8; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication Requires PIV
Data Layer	Hibernate	**Other**	

Replay

Replay- Inspection Processes Division			
Replay is used in the land and air environments to record actions taken by officers on the field using applications implementing replay to be a source of information for reviewing security officers.			
Key Facts			
Customer Transactions	N/A	**Data**	Images of screens that record user's activities

Replay- Inspection Processes Division			
Primary Stakeholders	Office of Professional Responsibility	**Current Hosting Environment**	NDC
Major Interfaces	TECS	**Application Age**	
Amplifying Business Information			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Servlets; Spring MVC; Application Type - Thick Client; Swing	**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse; Java 1.8
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV; Authentication Requires AD
Data Layer	MyBATIS; Data Type - Binary; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB; Hibernate; JDBC; Spring	**Other**	

Simplified Arrival (SA)

Simplified Arrival – Inspection Processes Division
Simplified Arrival (SA) is a new and innovative approach that incorporates advanced facial recognition technologies into the primary inspection to facilitate and expedite the entry process. The new Simplified Arrival application will eventually replace TPAC and TPAC-Face. Simplified Arrival leverages facial recognition technologies in order to facilitate and expedite the processing of arriving passengers and airline crew while enhancing security. Capturing facial biometrics of all passengers adds additional security, as currently there is no biometric verification of U.S. Citizens, most Canadians, citizens of a few other countries and travelers who are exempted for other reasons such as age and class of admission. Using facial matching as the primary biometric verification modality provides a previously unavailable method to verify and facilitate travel for almost everyone, not just those travelers for whom DHS has fingerprints. The Simplified Arrival process for air travel is the following: • The flight lands • The passenger heads to the entry lane • The passenger approaches the booth • The photo is captured and submitted to the facial matching service • The best photo match from DHS holdings is returned with a pointer to the associated manifest data • The officer verifies the match and continues the inspection process using the Simplified Arrival

Simplified Arrival – Inspection Processes Division			
Simplified Arrival provides the following benefits: • Improves upon TPAC/TPAC-Face; Eventual replacement • Replaces document scan with facial recognition • Bypasses fingerprint capture for travelers whose good quality fingerprints are on file • Integrates 1:1 facial comparison for first time Visa Waiver Program (VWP) travelers • Compares captured photo with travel document/eChip photo			
Key Facts			
Customer Transactions	Simplified Arrival-Air is currently deployed in all primary lanes and being used 100% in San Diego. Approximately 500 transactions processed per day in SA AIR.	**Data**	SA calls PIP, PQS and the Biometric services which maintain data.
Primary Stakeholders	CBPOs, air travelers, pedestrian land travelers	**Current Hosting Environment**	NDC
Major Interfaces	OBIM, PIP, PQS and Biometric Services. TVS is called via the PIP service.	**Application Age**	New.
Amplifying Business Information			
Currently deployed at 3 ports: Dulles, Miami, San Diego			
Key Technologies			
Presentation Layer	React, Java 1.8, .NET C++, AngularJS, Spring	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise, Windows 10	**IDE**	Eclipse
Middleware	Tomcat, WebLogic Server 12.1	**Security Layer/ Authentication**	Authentication - TECS OUD; Authentication Requires PIV
Data Layer	Data Type - Binary; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB; Data Type – Other Data Type – XML	**Other**	

System Support and User Profile Processing (SSUP)

System Support and User Profile processing (SSUP) – Interfaces and Support Processes Division
System Support (SS) is system support functions such as defining workstations, used primarily by PSPD SysTech. User Profile (UP) are user profile functions for things like adding users and resetting passwords.
Key Facts

System Support and User Profile processing (SSUP) – Interfaces and Support Processes Division			
Customer Transactions	Approx. 1K/day	**Data**	Oracle 1 GB Growth 25% annually
Primary Stakeholders	OIT OFO Officers Participating Government Agencies	**Current Hosting Environment**	NDC
Major Interfaces	OUD, AD, BEMS/Bear	**Application Age**	2 years
Amplifying Business Information			
Supports CBP mission by providing formatted documentation of incidents.			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS / ICAM OUD; Authentication uses AD for SSO
Data Layer	MyBATIS; Hibernate Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

TECS Portal (application)

TECS Portal – Interfaces and Support Processes Division			
TECS Portal is the modernized gateway to functions that were formerly performed in Legacy TECS. The Portal itself is the anchor, from which other functions may be launched and executed, that sustain today's law enforcement and traveler screening capabilities. The Portal and all the functions available through it have, as a whole, become known as "TECS Portal." TECS Portal is the gateway to the modernized TECS functions, and provides easy access to them, such as drop-down menu selections or "favorites" saved by system users. Functions available on the web vs. mainframe have been exploited to enhance the user experience where possible, such as providing photos when available or applicable.			
Key Facts			
Customer Transactions	Approx. 50K/day	**Data**	Oracle 1GB, Growth 10%/annual
Primary	CBP Field Operations,	**Current**	NDC

TECS Portal – Interfaces and Support Processes Division			
Stakeholders	Border Patrol, and Air and Marine; Immigration and Customs Enforcement 27 Federal agencies 11 DHS Components	**Hosting Environment**	
Major Interfaces	N/A. Portal is an access point for other applications.	**Application Age**	5 Years

Amplifying Business Information

Performance Monitoring Parameters for TECS Portal User Profile functions:

Function	Objective	Threshold	Below Threshold
Login	<3 secs	3-5 secs	>5 secs
Get UP	<3 secs	3-5 secs	>5 secs
Get Sel UP	<3 secs	3-5 secs	>5 secs
Create UP	<3 secs	3-5 secs	>5 secs
Save UP	<3 secs	3-5 secs	>5 secs
Search	<3 secs	3-5 secs	>5 secs

Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; JQuery 1.6.2; JSF; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires AD
Data Layer	MyBATIS; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

TECS Screening Services (TSSV)

TECS Screening Services (TSSV) – Interfaces and Support Processes Division
TECS Screening Services (TSSV) is the integration tier under Lookout Records and Data Services track in the TECS MOD program. It has been designed and implemented to replace the existing TECS Messaging Query Interface (TMQI) interfaces. TSSV is the gateway for systems-to-systems query interfaces that are external to Passenger Systems Program Directorate (PSPD). TSSV's high-level business objectives align with CBP's and the Department of Homeland Security's (DHS) mission to be the guardian of our Nation's borders and core value of vigilance through the efficient processing of queries for TECS, SEACATS, Federal Bureau of Investigation (FBI) NCIC, FBI III, Nlets, Interpol and RMAS databases.

TECS Screening Services (TSSV) – Interfaces and Support Processes Division			
TSSV provides the following benefits: • Interfaces for both external and internal consumers • Audit logging at message ingress and egress • System or user authorization via modernized Security Authorization Service • Message processing monitoring and metrics recording			
Key Facts			
Customer Transactions	51,000,000 requests conducted in August 2018 9,100,000 responses conducted in August 2018	**Data**	Oracle 18 TBs Growth: 10%
Primary Stakeholders	TECS queries (i.e., Subject Records, Incident Log, Travel Documents, Secondary Inspections) Seized Assets and Cases Tracking System (SEACATS) National Crime Information Center (NCIC), The International Justice and Public Safety Network (Nlets) and Interstate Identification Index (III) queries Interpol and Regional Movement Alert System (RMAS) queries Interpol query for lost and stolen passports	**Current Hosting Environment**	NDC
Major Interfaces	U.S. Citizenship and Immigration Services (USCIS) Person Centric Query Service (PCQS/RFSS) USCIS Authorization Token Layer Acquisition Service (ATLAS) Interface Immigration and Customs Enforcement (ICE) Case Management (QICE) RMAS Broker Interface (RMAS) Customs and Border Protection (CBP) Vetting (TOSF/TOSQ) CBP Manifest RMAS Interface (MFST) CBP Global Enrollment Trusted Worker (GTWS/GTWR) CBP Electronic System for Travel Authorization (ESTA) CBP Electronic Visa Update System (EVUS) CBP Targeting & Analysis Systems Program Directorate (TASPD) Targeting Framework (TFSI/TFSV/TFAL/TFSU) CBP TECS Profile Service (GES/CBPV/TASPD/ICE)	**Application Age**	6+ years old
Amplifying Business Information			
At a high level, TSSV provides functionalities with Extensible Markup Language (XML), or string formats via as Message Queue (MQ), or web service interface. There are 73 query types consumers can run.			

TECS Screening Services (TSSV) – Interfaces and Support Processes Division			
Key Technologies			
Presentation Layer		**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication Requires SSO
Data Layer	Spring; Data Type - Char; Data Type - BLOB	**Other**	

Terms, Acronyms, and Definitions (TAD)

TERMS, Acronyms, and Definitions (TAD) – Interfaces and Support Processes Division			
Terms, Acronyms, and Definitions (TAD) is a central repository of terms, acronyms, abbreviations, initials, and definitions for Customs and Border Protection (CBP). TAD provides centrally located repository that is accessible via the intranet to query, modify, delete, or add acronyms/definitions for terms used within DHS, CBP, or the federal government as a whole.			
Key Facts			
Customer Transactions	Minimal	**Data**	
Primary Stakeholders	Any CBP contractor or federal employee with access to the CBP intranet.	**Current Hosting Environment**	NDC
Major Interfaces	None	**Application Age**	10+ years old
Amplifying Business Information			
Key Technologies			
Presentation Layer	Application Type - Web App; HTML5/JavaScript; Spring MVC	**Backend Components**	Deployment Artifacts - WAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; JavaScript; Eclipse
Middleware	Application Type - Service App; WebLogic	**Security Layer/ Authentication**	Authentication – TAD Database
Data Layer	MyBATIS; Spring; Data Type - JSON; Data Type - CLOB;	**Other**	

Travel Documents and Encounter Data (TDED)

Travel Documents and Encounter Data (TDED)– Interface and Support Processes Division
Travel Documents and Encounter Data (TDED) is the consolidated repository for travel documents (passports, visas, Legal Permanent Resident cards, Enhanced Driver's Licenses, etc.) and encounter data (border crossings) for passengers and conveyances. TDED maintains over 40 interfaces for data ingestion and transmission, and is the system of record for travel documents within DHS. TDED provides services for Primary and Secondary applications, and maintains multiple query pages on the TECS Portal website. TDED provides quick and easy interfaces via TECS Portal for officers to perform travel document, encounter data, CMIR, I-94, and I736 queries. TDED also maintains several key back-end services that other applications use for system-to-system queries. TDED supports the CBP mission by providing a central repository of travel documents, arrivals and departures, and I94s. Numerous applications query TDED's data holdings in real-time. Additionally, because TDED maintains the photo associated with a travel document, various facial matching initiatives are using TDED's photos to compose a photo gallery for an individual traveler.

Key Facts			
Customer Transactions	For Travel Doc Services, the volume is approximately 10,000 calls per minute For I-94, CMIR and Encounter Services, the volume is approximately 2,000 calls per minute	**Data**	Two Oracle databases: Travel Document – 16 TBs Encounter – 20 TBs
Primary Stakeholders	Any TECS Portal user (e.g., CBP, ICE, USCIS, TSA, FBI, etc.). The TECS Primary applications, Manifest, TECS Portal, EVUS, APC, PDS and ADIS are all consumers of the TDED Travel Document Service.	**Current Hosting Environment**	NDC
Major Interfaces	DoS, FBI, Dept. of Treasury, Dept. of Commerce, U.S. Selective Service, FBI FTTTF, states with Enhanced Driver's Licenses, tribes using Enhanced Tribal Cards	**Application Age**	5 years

Amplifying Business Information

TDED maintains the following travel documents:

- U.S. Passports - 257,726,602*
- Non-U.S. Passports - 89,247,992
- Immigrant Visas - 8,888,329
- Non-Immigrant Visas - 148,050,729
- Legal Permanent Resident (LPR) cards - 45,272,712
- Enhanced Driver's Licenses (EDLs)
- Enhanced Tribal Cards (ETCs) - 5,478,348 (EDLs and ETCs combined)

* All numbers are as of August 31, 2018.

- 200,000 U.S. passports received by TDED each day from the Department of State
- 1.3 billion I-94s processed since 1983
- 12 billion person and vehicle encounters (crossings)
- 144 million Non-immigrant visas processed since 1996
- TDED is used in Secondary to research admissibility of travelers, or goods
- TDED also provides links to other systems to facilitate both gathering and recording additional information such as Person Lookout data, incident logs, Manifest Data and more.

TDED response time objective: < 3 secs

Travel Documents and Encounter Data (TDED)– Interface and Support Processes Division			
TDED response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Application Type - Web App; JQuery 1.6.2; JSF; JSP; Servlets; Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Standalone JAR files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.6; Java 1.8; Eclipse; Java 1.6; Java 1.7; Java 1.8
Middleware	Application Type - Service App; WebLogic; WebSphere; WebSphere MQ	**Security Layer/ Authentication**	Authentication - Top Secret-LDAP; Authentication - TECS CAS
Data Layer	Hibernate; JDBC; MyBATIS; Spring; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB; Data Type - Binary	**Other**	

TDED Currency and Monetary Instruments Report (CMIR)

TDED Currency and Monetary Instruments Report (CMIR) – Interfaces and Support Processes Division			
The Travel Documents and Encounter Data (TDED) Currency and Monetary Instruments Report (CMIR) Service (SOAP) provides consumer applications the ability to query CMIR forms. A CMIR is a Currency and Monetary Instrument Report, also called a FinCEN Form 105. This form is required to be completed by anyone entering or departing the U.S. with more than $10,000 in monetary instruments (cash, checks, bonds, etc.). CBP Officers at the ports of entry collect the paper forms and either scan or mail them to a data entry contractor that keys in the data on the forms and sends it to TDED.			
Key Facts			
Customer Transactions	Approximately 2,000 calls per minute	**Data**	Oracle Encounter Database • 7,411,253 records Receive about 600/day or 18,000/month
Primary Stakeholders	TECS Portal is the only consumer of the TDED CMIR Service. Users of the TECS Portal CMIR page are able to query submitted CMIR forms for review.	**Current Hosting Environment**	NDC
Major Interfaces	Dept. of Treasury, FinCEN TECS Portal UI Coleman Data Solutions (CMIR data entry contractor)	**Application Age**	Approx. 5 years
Amplifying Business Information			
The TDED CMIR Service supports the CBP mission by allowing TECS Portal users to query and review traveler, business and financial information collected on the FinCEN Form 105. These data are also shared with the Dept. of Treasury FinCEN program.			

TDED Currency and Monetary Instruments Report (CMIR) – Interfaces and Support Processes Division			
TDED response time objective: < 3 secs TDED response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Service Interface – SOAP Web Service	**Backend Components**	Deployment Artifacts - EAR Files JDK1.8 Spring Framework
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse, SQL Developer, SOAP UI MQExplorer
Middleware	WebLogic; WebSphere MQ Kafka (still in QAX)	**Security Layer/ Authentication**	SSL
Data Layer	MyBatis Persistence Framework Oracle DB Data Type - Char Data Type - CLOB Data Type - BLOB Data Type - Binary	**Other**	

TDED Encounter Service (Query)

TDED Encounter Service (Query) – Interfaces and Support Processes Division			
The TDED Encounter Service (SOAP) allows other applications to query encounter records (aka border crossings), dating back to 1983 (when TECS was created).			
Key Facts			
Customer Transactions	Approximately 2,000 calls per minute	**Data**	Not applicable
Primary Stakeholders	TECS Portal is the only application that uses the Encounter Service. TECS Portal users can perform an Encounter History Query to view travel history for users. The UI allows for exact name matching and also wildcard searches on last name.	**Current Hosting Environment**	NDC
Major Interfaces	TECS Portal (UI)	**Application Age**	Approx. 5 years
Amplifying Business Information			
The TDED Encounter Service supports TECS Portal users by providing access to the arrivals and departures of individuals traveling into and out of the United States. TDED response time objective: < 3 secs TDED response time threshold: 3-5 secs			
Key Technologies			

TDED Encounter Service (Query) – Interfaces and Support Processes Division			
Presentation Layer	Service Interface – SOAP Web Service	**Backend Components**	Deployment Artifacts - EAR Files JDK1.8 Spring Framework
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse, SQL Developer, SOAP UI MQExplorer
Middleware	WebLogic; WebSphere MQ Kafka (still in QAX)	**Security Layer/ Authentication**	SSL
Data Layer	MyBatis Persistence Framework Oracle DB Data Type - Char Data Type - CLOB Data Type - BLOB Data Type - Binary	**Other**	

TDED I94 Service (Create, Update, Delete, Query)

TDED I94 Service (Create, Update, Delete, Query) – Interfaces and Support Processes Division			
The TDED I94 Service (SOAP) allows PSPD applications to query, create, update and delete ("CRUD") I94 records.			
Key Facts			
Customer Transactions	Approximately 2,000 calls per minute	**Data**	Not applicable
Primary Stakeholders	TECS Portal and the Primary applications are consumers of the I94 Service. Most I94s are generated automatically by Primary applications such as TPAC when the traveler is admitted into the United States.	**Current Hosting Environment**	NDC
Major Interfaces	Primary applications (TPAC, VPC, etc.) TECS Portal (UI) Coleman Data Solutions (Paper I-94 data entry contractor)	**Application Age**	Approx. 5 years
Amplifying Business Information			
The TDED I94 Service supports the CBP mission of I94 automation. Today, paper-based I94s are a very small percentage of the total number of I94s issued, and continue to go down in number. Eventually, nearly 100% of I94s will be created / issued using the TDED I94 Service. TDED response time objective: < 3 secs TDED response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Service Interface – SOAP Web Service	**Backend Components**	Deployment Artifacts - EAR Files

TDED I94 Service (Create, Update, Delete, Query) – Interfaces and Support Processes Division			
			JDK1.8 Spring Framework
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse, SQL Developer, SOAP UI MQExplorer
Middleware	WebLogic; WebSphere MQ Kafka (still in QAX)	**Security Layer/ Authentication**	SSL
Data Layer	MyBatis Persistence Framework Oracle DB Data Type - Char Data Type - CLOB Data Type - BLOB Data Type - Binary	**Other**	

TDED Provisional I94 Service (Create, Query)

TDED Provisional I94 Service (Create, Query) – Interfaces and Support Processes Division			
The TDED Provisional I-94 Service (SOAP) allows PSPD applications to create and query provisional I-94s. A provisional I-94 allows travelers to apply and pay for their I-94 online prior to arriving at a land port of entry. Travelers can speed up their entry into the U.S. by providing their biographic and travel information, and paying the $6 fee for their I-94 application online up to seven days prior to their entry.			
Key Facts			
Customer Transactions	Approximately 2,000 calls per minute	**Data**	Not applicable
Primary Stakeholders	The I-94 Public Website (https://i94.cbp.dhs.gov/I94/#/home) and the Primary applications are consumers of the Provisional I-94 Service. The public website is where travelers apply for the provisional I-94. Upon submitting the request, the website calls the TDED Provisional I-94 Service to create the provisional I-94 in the TDED database.	**Current Hosting Environment**	NDC
Major Interfaces	Primary applications (TPAC, VPC, etc.) Public-facing I-94 website	**Application Age**	Approx. 5 years
Amplifying Business Information			
The TDED Provisional I-94 Service supports the CBP mission of facilitating legitimate travel. CBP is always looking at how to use technology and automation to make the travel experience easier and more efficient for individuals. TDED response time objective: < 3 secs TDED response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Service Interface – SOAP Web Service	**Backend Components**	Deployment Artifacts - EAR Files

TDED Provisional I94 Service (Create, Query) – Interfaces and Support Processes Division			
			JDK1.8 Spring Framework
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse, SQL Developer, SOAP UI MQExplorer
Middleware	WebLogic; WebSphere MQ Kafka (still in QAX)	**Security Layer/ Authentication**	SSL
Data Layer	MyBatis Persistence Framework Oracle DB Data Type - Char Data Type - CLOB Data Type - BLOB Data Type - Binary	**Other**	

TDED I-736 Service (Create, Update, Query)

TDED I-736 Service (Create, Update, Query) – Interfaces and Support Processes Division			
The TDED I-736 Service is a RESTful service used by TECS Portal and the I-736 Public Website (https://i736.cbp.dhs.gov/I736/#/home) to create, update and query I-736s. Citizens or nationals from one of the twelve countries participating in the Guam and Commonwealth of Northern Marianas Islands (CNMI) visa waiver program (Australia, Brunei, Hong Kong, Japan, Malaysia, Nauru, New Zealand, Papua New Guinea, South Korea, Singapore, Taiwan and the United Kingdom) who travel to Guam or CNMI are required, with a few exceptions, to present a signed paper copy of the I-736 form upon arrival.			
Key Facts			
Customer Transactions	Approximately 2,000 calls per minute	**Data**	Not applicable
Primary Stakeholders	The public-facing I-736 website (https://i736.cbp.dhs.gov/I736/#/home) and TECS Portal are consumers of the TDED I-736 Service.	**Current Hosting Environment**	NDC
Major Interfaces	TECS Portal (UI) Public-facing I-736 website	**Application Age**	1 year
Amplifying Business Information			
The TDED I-736 Service supports the CBP mission of facilitating legitimate travel. CBP is always looking at how to use technology and automation to make the travel experience easier and more efficient for individuals. The TDED I-736 Service supports the CBP mission by allowing travelers to Guam or the CNMI to apply for their I-736 online. The service also allows TECS Portal users to query and update submitted I-736 forms. TDED response time objective: < 3 secs TDED response time threshold: 3-5 secs			
Key Technologies			
Presentation Layer	Service Interface – REST Web Service	**Backend Components**	Deployment Artifacts - WAR Files

TDED I-736 Service (Create, Update, Query) – Interfaces and Support Processes Division			
			JDK1.8 Spring Boot Framework
OS Layer	Red Hat Linux Enterprise	**IDE**	Eclipse, SQL Developer, SOAP UI
Middleware	WebLogic/Docker Container in AWS	**Security Layer/ Authentication**	SSL
Data Layer	MyBatis Persistence Framework Oracle DB Data Type - Char	**Other**	

Traveler Primary Arrival Client (TPAC)/TPAC-Face Pilot

Travel Primary Arrival Client (TPAC/TPAC-Face Pilot – Inspection Processes Division
The Traveler Primary Arrival Client (TPAC) application is used to assist with the screening of travelers as they arrive at air and sea ports-of-entry (POEs) seeking entry into the United States. TPAC-Face Pilot is to demonstrate the technical capability and operational impact of leveraging facial recognition technologies in order to facilitate and expedite the processing of arriving passengers and airline crew while enhancing security. Capturing facial biometrics of all passengers adds additional security, as currently there is no biometric verification of U.S. Citizens, most Canadians, citizens of a few other countries and travelers who are exempted for other reasons such as age and class of admission. Using facial matching as the primary biometric verification modality provides a previously unavailable method to verify and facilitate travel for almost everyone, not just those travelers for whom DHS has fingerprints. The TPAC-Face Pilot is the first phase of a technology demonstration of the Simplified Arrival process at select international airports. It incorporates advanced facial recognition biometrics technologies into the existing TPAC functionality. TPAC-Face provides the following benefits: • Replaces document scan with facial recognition • Bypasses fingerprint capture for travelers whose good quality fingerprints are on file • Integrates 1:1 facial comparison for first time Visa Waiver Program (VWP) travelers • Compares captured photo with travel document/eChip photo Current Process: • The flight lands • The passenger heads to the entry lane • The passenger presents his/her travel document • The officer scans it • Biographic data from the travel document is used to search the manifest • The officer verifies the manifest match and continues the inspection process TPAC-Face Pilot Process: • The flight lands • The passenger heads to the entry lane • The passenger approaches the booth • The photo is captured and submitted to the facial matching service • The best photo match from DHS holdings is returned with a pointer to the associated manifest data • The officer verifies the match and continues the inspection process

Travel Primary Arrival Client (TPAC/TPAC-Face Pilot – Inspection Processes Division			
Key Facts			
Customer Transactions	TPAC processes approximately 250, 000 transactions a day (includes TPAC Face)	**Data**	Interfaces with PIP, PQS and the Biometric services for data services.
Primary Stakeholders	TPAC is used at over 400 POEs and other sites for processing air and sea travelers. TPAC Face is used by CBP Office of Field Operations in 14 ports of entry: Atlanta, Aruba, Dublin, Dulles, Ft Lauderdale, Houston, JFK, Los Angeles, Las Vegas, Miami, Orlando, San Diego, San Jose, Shannon.	**Current Hosting Environment**	NDC
Major Interfaces	OBIM, SEVIS, PIP, PQS and Biometric Services Also calls TVS through the PIP service	**Application Age**	TPAC (10 years old), Biometric capability added to TPAC (TPAC-Face) in October 2017

Amplifying Business Information

Performance Monitoring Parameters:

Function	Objective	Threshold	Below Threshold
Login	<3 secs	3-5 secs	>5 secs
PIP Manifest	<3 secs	3-5 secs	>5 secs
PIP Facial 1:N	<3 secs	3-5 secs	>5 secs
PIP Facial 1:1	<3 secs	3-5 secs	>5 secs
IDENT: Pre-Verify Bio	<20 secs	20-30 secs	>30 secs
IDENT: Verify 4	<20 secs	20-30 secs	>30 secs
IDENT: Identify 10	<20 secs	20-30 secs	>30 secs
PQS TECS Hit Query	<3 secs	3-5 secs	>5 secs
PIP NCIC	<3 secs	3-5 secs	>5 secs
PIP Encounter	<3 secs	3-5 secs	>5 secs
ICE SEVIS	<3 secs	3-5 secs	>5 secs
TDED US Passport	<3 secs	3-5 secs	>5 secs
ESTA	<3 secs	3-5 secs	>5 secs
EVUS	<3 secs	3-5 secs	>5 secs
GES	<3 secs	3-5 secs	>5 secs

TPAC is targeted for retirement to be replaced by Simplified Arrival.

Key Technologies			
Presentation Layer	Application Type - Thick Client; Swing	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Standalone JAR files; Deployment Artifacts - Database Scripts

Travel Primary Arrival Client (TPAC/TPAC-Face Pilot – Inspection Processes Division			
OS Layer	Red Hat Linux Enterprise; Windows	**IDE**	Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	
Data Layer	EJB2; JDBC; Spring; Data Type - Binary; Data Type - Char; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	

Trusted Traveler Programs System (TTP)

Trusted Traveler Programs (TTP) – I-Solutions Division			
The Trusted Traveler Program (TTP) is Customs and Border Protection's (CBP) first public-facing cloud based internet application that facilitates the enrollment into the Global Entry (GE), NEXUS, Secure Electronic Network for Traveler Rapid Inspection (SENTRI), and Free and Secure Trade (FAST) Programs, featuring: • Seamless website navigation • Self-creation and management of user account information using LOGIN.GOV • Simple online application process • Monitor application and enrollment status online • Online payment of application fee • Streamlined, easy-to-use, interview appointment scheduling function • Mobile friendly website • User-managed Password Reset • Online Trusted Traveler card activation The TTP website allows travelers to easily submit an application, submit payment, activate travel card, and schedule appointments for GE, NEXUS, SENTRI, and FAST Programs. Conditionally Approved travelers can now complete GE enrollment upon entry into the U.S. at an Enrollment on Arrival Center. Program enrollment provides expedited travel for pre-approved, low-risk travelers through dedicated lanes and kiosks. TTP pushes the zone of security outward and advances the department and agency goals of securing the U.S			
Key Facts			
Customer Transactions	In the first year, there were over 1,594,209 new applications, an average of 4,648 per day, and 23,819,869 successful logins; an average of 69,446 per day. The first year has generated more than 184,114,875 million in revenue.	**Data**	913 GBs
Primary Stakeholders	Public users, including U.S. citizens and non-U.S. citizens.	**Current Hosting Environment**	CBP AWS Cloud East (CACE)
Major Interfaces		**Application Age**	1 Year
Amplifying Business Information			
There are more than 8,058,554 active TTP members.			
Key Technologies			

Trusted Traveler Programs (TTP) – I-Solutions Division			
Presentation Layer	Application Type - Web App; Angular	**Backend Components**	Deployment Artifacts - Java Docker containers Deployment Artifacts - Database Scripts
OS Layer	Centos Linux, Docker container	**IDE**	Atom, Visual Studio Community Edition (UI) Eclipse (Backend) MySQL Workbench (DB)
Middleware	Application Type - Service App; Spring Boot, Tomcat	**Security Layer/ Authentication**	Public 2 factor Authentication – Login.gov CBP Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires PIV
Data Layer	Spring Data Rest, JPA; Hibernate, MySQL Data Type - Char; Data Type – JSON; Data Type – XML	**Other**	

US Arrival (Application)

US Arrival (Application) – Inspection Processes Division
The US Arrival application enables electronic capture of arrival data (biographic and class of admission) for travelers who are issued I-94 and I-94W forms. These forms are also called permits. It complies with the initiative to collect the fingerprints of each traveler as they enter the United States. This capability will improve the recording and unique identification of travelers at our nation's land border ports of entry (POEs), and provide the foundation for future security. US Arrival is currently used only at land borders. US Arrival allows the user to query I-94 and I-94W documents used at the border by foreign nationals to enhance national security and ensure the integrity of our immigration system. US Arrival was created to collect, maintain, and share information on foreign nationals in order to enhance national security, facilitate legitimate trade and travel, and ensure the integrity of our immigration system. The functionality of the US Arrival application: • Enables the electronic capture of arrival data (biographic and class of admission) for travelers who are issued Form I-94 and Form I-94W • Prints Form I-94 and electronically generates admission number • Electronically generates the I-94W numbers on the traveler's departure stub • Sends crossing data to TECS and the Arrival and Departure Information System (ADIS) • Permits arrival data to be shared with other authorized end users • Utilizes biographics for traveler verification • Supports the Entry Exit initiative with the Canadian Border Services Agency (CBSA) • Supports Electronic Visa Update System (EVUS) and Student and Exchange Visitor Information System (SEVIS) queries • Query Data captured from: • Machine Readable Zone (MRZ) cards, • ePassports, or • Manual entry via the keyboard

Key Facts			
Customer Transactions	Average 8,500 a day	**Data**	Admission records and I-94s

US Arrival (Application) – Inspection Processes Division			
Primary Stakeholders	US Arrival is used by Customs and Border Protection (CBP) Officers and is in use at the majority of the northern and southwest border ports of entry.	**Current Hosting Environment**	NDC
Major Interfaces	TECS Primary Query Service (PQS) Primary Inspection Process (PIP) Office of OBIM Identity (OBIM)	**Application Age**	Approximately 9 years old

Amplifying Business Information

Performance Monitoring Parameters:

Function	Objective	Threshold	Below Threshold
PIP Login	<3 secs	3-5 secs	>5 secs
PIP Person Query	<3 secs	3-5 secs	>5 secs
PIP NCIC	<3 secs	3-5 secs	>5 secs
IDENT: Verify 4	<20 secs	20-30 secs	>30 secs
IDENT: Identify 10	<20 secs	20-30 secs	>30 secs

US Arrival is targeted for retirement.

Key Technologies			
Presentation Layer	Application Type - Thick Client; Spring MVC	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Enterprise Linux 7	**IDE**	Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication Requires PIV
Data Layer	EJB2; EJB3; Hibernate; JDBC; Spring; Data Type - Char; Data Type - BLOB	**Other**	

Vehicle Primary Client (VPC)

Vehicle Primary Client (VPC)– Inspection Processes Division

The Vehicle Primary Client (VPC) application is used to screen travelers and their privately-owned vehicles (POVs) as they arrive at land border ports of entry (POEs) seeking entry into the United States.

VPC captures, displays, and stores information about land travelers and their vehicles. It initiates queries to TECS, the National Crime and Information Center (NCIC), the International Justice and Public Safety Network (Nlets), and the Automated Targeting System (ATS) then provides the query results to the officers working on Primary inbound lanes to help in determining traveler and vehicle admissibility. At the end of the officer interview, the application packages all data and photos captured, then this information is stored as a package for future reference. The information includes both data entered by the officers and information captured by the pre-primary lane equipment (document and license plate reads, and photos taken). This process ensures that the full package of information is available to Secondary if additional traveler/vehicle screening is required.

Vehicle Primary Client (VPC)– Inspection Processes Division

VPC supports the work of the CBP officers and United States Border Patrol (USBP) agents via TECS, NCIC, Nlets, and ATS queries to ensure both vehicles and their occupants are fully vetted for admissibility into the United States.

Outbound Primary Client (OPC) is a sister application of VPC that is used by CBP officers at land border ports in the outbound lanes. OPC is targeted for retirement.

Border Patrol Client (BPC) is used at traffic checkpoints along highways leading from border areas, conducting city patrol and transportation check, and anti-smuggling investigations to reduce the likelihood that dangerous people and capabilities enter the USA between the ports of entry. BPC is targeted for retirement.

Vehicle Primary Application and Integration Services (VPAIS) is the backend service providing vehicle primary services required to package and associate vehicle and traveler data used by Vehicle Primary Client application.

Land Primary Application and Integration Services (LPAIS) – Provides traveler data to VPAIS for VPC.

Key Facts

Customer Transactions	Approximately 490,000 Travelers a day Approximately 307,000 Incoming Privately Owned Vehicles a day	**Data**	Traveler border crossing and vehicle data
Primary Stakeholders	VPC is utilized by Customs and Border Protection at Users (CBP) officers working in inbound, primary lane booths at land border ports of entry (POE)	**Current Hosting Environment**	NDC
Major Interfaces	TECS Primary Query Service (PQS) Primary Inspection Process (PIP) Land Border Integration RFID and License Plate Readers GES	**Application Age**	Approximately 10 years old

Amplifying Business Information

Performance Monitoring Parameters:

Function	Objective	Threshold	Below Threshold
PIP Login	<3 secs	3-5 secs	>5 secs
PIP Person Query	<3 secs	3-5 secs	>5 secs
PIP NCIC Person Query	<3 secs	3-5 secs	>5 secs
PIP Vehicle Query	<3 secs	3-5 secs	>5 secs
PIP NCIC Vehicle Query	<3 secs	3-5 secs	>5 secs
GES RFID	<3 secs	3-5 secs	>5 secs
GES Vehicle	<3 secs	3-5 secs	>5 secs
PQS Admit Vehicle	<3 secs	3-5 secs	>5 secs

VPAIS is targeted for retirement.

Key Technologies VPC (frontend)

Vehicle Primary Client (VPC)– Inspection Processes Division			
Presentation Layer	Application Type - Thick Client; Spring MVC; Swing	**Backend Components**	Deployment Artifacts - EAR Files
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.7; Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires PIV
Data Layer	EJB2; EJB3; Hibernate; JDBC; Spring; Data Type - Binary; Data Type - Char	**Other**	
Key Technologies Outbound Primary Client (OPC)			
Presentation Layer	Application Type - Thick Client; Swing	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.7; Java 1.8; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires PIV
Data Layer	EJB2; EJB3; Hibernate; JDBC; Spring; Data Type - Binary; Data Type - Char; Data Type - BLOB	**Other**	
Key Technologies Border Patrol Client (BPC)			
Presentation Layer	Application Type - Thick Client; HTML5/JavaScript; Spring MVC; Swing	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - WAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; Eclipse
Middleware	WebLogic; WebSphere MQ	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires PIV
Data Layer	EJB2; EJB3; Hibernate; JDBC; Spring; Data Type - Char; Data Type - BLOB	**Other**	
Key Technologies VPAIS (backend)			
Presentation Layer	Application Type - Thick Client; Spring MVC; Swing	**Backend Components**	Deployment Artifacts - EAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.7; Java 1.8; JavaScript; Eclipse
Middleware	WebLogic	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires PIV

Vehicle Primary Client (VPC)– Inspection Processes Division			
Data Layer	EJB2; EJB3; Hibernate; JDBC; Spring; Data Type - Binary; Data Type - Char; Data Type - BLOB	**Other**	Deployment Artifacts - EAR Files; Deployment Artifacts - Database Scripts

Watch List Service (WLS)

WATCH LIST SERVICE (WLS) – Interfaces and Support Processes Division			
The Department of Homeland Security (DHS) Watchlist Service (WLS) is designed to automate and streamline the dissemination of pertinent Watchlist information from the Terrorist Screening Center (TSC) of the Department of Justice (DOJ) to components of DHS. Prior to the implementation of WLS, DHS Components received Watchlist data from the TSC through a variety of manual processes.			
Key Facts			
Customer Transactions	Watch list data, varies according to the scenarios	**Data**	Oracle WLSTECS: 2.13 TBs WLS: 6.25 TBs CBPV (part of WLS) 0.044 TBs NNSVREVET (part WLS) 0.65 TBs
Primary Stakeholders	DHS Screening Coordination Office (SCO) WLS Customs and Border Protection DHS Components	**Current Hosting Environment**	NDC
Major Interfaces		**Application Age**	10 years
Amplifying Business Information			
The WLS supports the “One DHS” information sharing directives. It utilizes Terrorist Watchlist Person Data Exchange Standard (TWPDES) to send and receive information.			
Key Technologies			
Presentation Layer	N/A	**Backend Components**	Deployment Artifacts - WAR Files; Deployment Artifacts - Database Scripts
OS Layer	Red Hat Linux Enterprise	**IDE**	Java 1.8; Eclipse
Middleware	Application Type - Service App; DataPower; WebLogic; WebSphere; WebSphere MQ	**Security Layer/ Authentication**	Authentication - TECS CAS; Authentication Requires SSO; Authentication Requires AD
Data Layer	MyBATIS; Data Type - JSON; Data Type - CLOB; Data Type - BLOB	**Other**	TWPDES follows the standards of the National Information Exchange Model (NIEM). This ensures that the WLS will support DHS information sharing.