| DHS Major Information Systems - 2023 version | | |
|---|---|---|
| **Investment Name** | **System Name** | **System Description** |
| **Cybersecurity and Infrastructure Security Agency (CISA) Systems** | | |
| CISA - ISCP (Infrastructure Security Compliance) - CSAT (P) | CSAT - Chemical Security Assessment Tool | The Chemical Security Assessment Tool (CSAT) is an online portal that houses the surveys and applications facilities must submit to the Cybersecurity and Infrastructure Security Agency (CISA) to determine which facilities are considered high-risk under the Chemical Facility Anti-Terrorism Standards (CFATS). These surveys and applications include the Top-Screen survey, Security Vulnerability Assessment (SVA), Site Security Plan (SSP) and Personnel Surety Program (PSP). |
| CISA - National Cybersecurity Protection System (NCPS) (P) | National Cybersecurity Protection System | The National Cybersecurity Protection System (NCPS) is an integrated system-of-systems that delivers a range of capabilities across five service areas focusing on detection and protection in the .gov mission space and information sharing and risk auditing in the critical infrastructure and private industry mission space. The NCPS program delivers capabilities that assist in federal network defense and defend against today's threats, while collaborating to build more secure and resilient infrastructure for the future. These capabilities provide a technological foundation that enables Cybersecurity and Infrastructure Security Agency (CISA) to secure and defend the government information technology infrastructure of the Federal Civilian Executive Branch against advanced cyber threats. In addition to providing technology to secure and defend the Information Technology infrastructure of the Federal Civilian Executive Branch of government, the NCPS provides much of the infrastructure, tools and capabilities the CISA Cyber Security Division (CSD) needs to meet its mission. Threat Hunting (TH), Vulnerability Management (VM), and Operational Collaboration (OC) are part of CSD that provides 24/7 information sharing, analysis, and an incidentresponse center acting as the national nexus of cyber and communications integration for the Federal Government, Intelligence Community (IC), and law enforcement. TH, VM and OC share information with the public and private sectors to provide greater understanding of cybersecurity and communications situational awareness on vulnerabilities, intrusions, incidents, mitigations, and recovery actions. During cyber incidents, TH, VM and OC serve as the National Response Center (NRC), bringing the full capabilities of the Federal Government to bear in a coordinated manner with State, Local, Tribal and Territorial Government (SLTT), and public and private sector partners. The NCPS was developed by CISA in close collaboration with its interagency stakeholders. Development of NCPS capabilities relies on tight collaboration and integration with cross-federal stakeholders in order to support the defense of their underlying networks. Through these relationships, CISA can develop and deliver analytic products and real-time defensive services to better understand and manage risk to our critical infrastructure. This analysis provides valuable cyber incident information and generates situational awareness and decision support data that is used by incident response teams, governmental and critical infrastructure organizations, and national leadership. |

| | | |
|---|---|---|
| CISA - CISA Gateway (P) | CISA Gateway | The CISA Gateway serves as the single interface through which DHS mission partners access a broad range of integrated Infrastructure Protection (IP) tools, analytics, and information. This collection of tools, data, and capabilities allow mission partners to conduct comprehensive vulnerability assessments, visualizations, and risk analysis. |
| CISA - Critical Infrastructure Assessment and Reporting (CIAR) Program (P) | National Coordinating Center LAN Glebe Rd | The National Coordinating Center LAN (NCCLAN) is used by ERO/CISA Central Personnel to support the information sharing mission of the COMM-ISAC. This provides analysts access to local file sharing capabilities and access to mission-required software apps in an environment that allows for ERO/Industry proprietary information to be utilized for situational awareness. The research component of the NCC LAN aids in the research of Internet threats and vulnerabilities and supports of the analysis and research mission of the NCC-COMM -ISAC. Without impacting the ability of the ERO/CISA Central to support the NCC COMM-ISAC information sharing mission, the research capability provides timely situational awareness for developing circumstances that could escalate to NS/EP and ESF #2 and #14 events. |
| CISA ServiceNow | CISA ServiceNow | The CISA ServiceNow (C-SNOW) will leverage UWF ServiceNow CSAM ATO package. The new CSN CSAM package would provide a centralized and collaborative system for workflow tracking, request fulfillment, incident management, and customer relationship management across Cybersecurity and Infrastructure Security Agency (CISA) and support all Sub-Components within CISA using ServiceNow regarding security/privacy control, documentations, and compliance requirements. |
| CISA - National Cybersecurity Protection System (NCPS)(NCPS) | Cyberscope | The CyberScope web application supports an initiative by the Office of Management and Budget (OMB) to automate collection and reporting of Federal Information Security Management Act (FISMA) requirements from all Federal departments and agencies. CyberScope carries Sensitive but Unclassified (SBU) information, and supports approximately 135 reporting agencies.Within DHS, the FISMA reporting responsibility falls within the CyberSecurity and Infrastructure Security Agency (CISA) Office of Cybersecurity and Communications (CS&C). The Federal Network Resilience (FNR) Branch manages the program responsibility and the Network Security Deployment (NSD) Branch manages operational responsibility. CyberScope is an element within CS&C s National Cybersecurity Protection System (NCPS). In accordance with OMB Memorandum OMB 10-15 and OMB10-28, DHS was delegated with primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. 3543. This requirement resulted from Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other agency management needing various levels of FISMA data presented to them in ways that enable timely decision making. The agencies needed to automate security-related activities and acquire tools that correlate and analyze security-related information. The CyberScope application was designated for FISMA reporting for agencies. it is designed to follow a three-tiered approach: 1. Data feeds directly from security management tools 2. Government-wide benchmarking on security posture 3. Agency-specific interviews Cybersecurity and Infrastructure Security Agency (CISA) within DHS and the Office Management and Budget (OMB). DHS supports development of the CyberScope application and technical integration with reporting agencies. |

| | | |
|---|---|---|
| CISA - National Cybersecurity Protection System (NCPS) | Trusted Automated eXchange of Indicator Information server | The DHS TAXII Server, previously referred to as “FLARE”, “FLAREsuite”, or “FLAREsuite on AWS”, is designed to support shared situational awareness and collaboration across several cyber centers in a publish/subscribe model. The DHS TAXII Server is delivered via Amazon Web Services (AWS) GovCloud and is deployed in a secure General Services Administration (GSA)-approved Infrastructure as a Service (IaaS). |
| CISA - Bombing Prevention - TRIPwire | Technical Resource for Incident Prevention - Cloud | TRIPwire is an online information sharing resource on IED incidents, tactics, techniques, and procedures, as well as corresponding IED prevention and protective measures in order to better identify prevention opportunities involving improvised explosive devices (IEDs). TRIPwire provides information regarding the processes by which terrorist groups design, develop, manufacture, deploy, train with, and employ IEDs. TRIPwire enhances domestic preparedness by giving the nation’s security and emergency services professionals’ valuable information and resources to prevent, protect, respond to, and mitigate bombing incidents. Members of the portal are individually vetted by the TRIPwire help desk as valid users of the system. TRIPwire serves the bombing prevention community as a "one-stop resource" of consolidated and expert-validated resource of near real-time information on IEDs, relevant news, and threat alerts. TRIPwire also facilitates information sharing and networking by offering collaboration among members of the bombing prevention and response community. The community of interest served by the TRIPwire portal is law enforcement for the purpose bombing prevention. |
| CISA - FedHR Navigator (P) | CISA FedHR Navigator | The CISA FedHR Navigator is a Software as a Service (SaaS) system used to support the mission of Human Resource (HR) Specialists responsible for preparing employees' estimates of future retirement benefits and completing retirement packages for submission. The FedHR Navigator provides the capability for the HR Specialist to manually input employee files, or submit complete company lists, or request that EconSys download from the National Finance Center (NFC) employee information.  Additionally, FedHR Navigator provides Cyber Workforce Management: Automates the process by which CISA collects, tracks and validates cyber certification information related to CISA's cyber positions as part of CISA's Cybersecurity Pay Enhancements Program. This new function will also track employee eligibility for incentive pay based on associated CISA-cyber certifications. Performance Management: Provides case tracking and workflow to streamline performance management functions. Enables managers to create and approve Performance Plans and coordinates the Quarterly Review process. Case tracking allows for routing these documents for reviews and approvals. Future enhancements to this capability will include version control for Performance Plans. |
| **DHS Headquarters Systems** | | |

| | | |
|---|---|---|
| DHS - CIO - Homeland Security Information Network (HSIN) (P) | Homeland Security Information Network Cloud | HSIN servers as DHS' portal for information sharing within Federal, State, territory, local, and tribal governments. |
| **Federal Emergency Management Agency (FEMA) Systems** | | |
| FEMA - Data Center - Emergency Operations Center ITSC & Cloud (P) | FEMA Cloud Environment Amazon Web Services | The FCE AWS is an Infrastructure as a Service (IaaS) environment that will utilize a co-location provider that enables FEMA access to Amazon Web Services (AWS). A Cloud Access Point (CAP) is utilized and will allow connectivity between AWS and Mount Weather. |
| FEMA - Disaster Assistance Information Services (DAIS) (P) | Individual Assistance Survivor Online Application & Resources Portal | The SOAR system hosts the DisasterAssistance.gov web portal, a content management framework, a rules engine, and the registration intake capability that allow disaster survivors to apply for FEMA Individual Assistance and check the status of their application online, and get information about other Federal Agencies that might also provide assistance. SOAR also contains the Registration Intake capability used by FEMA's call center agents. |
| FEMA - Enterprise Data and Analytics Modernization Initiative (EDAMI) (P) | FEMA Data Exchange - Azure | FEMADex cloud based data warehouse allows FEMA to analyze and share data throughout the Agency, as well as with trusted partner. |

| | | |
|---|---|---|
| FEMA - Grants Management Modernization (P) | Streamlined Platform for Agile Release and Transformation Acceleration | The Streamlined Platform for Agile Release and Transformation Acceleration (SPARTA) system is the resulting environment of the Grants Management Modernization initiative. The purpose of SPARTA is to interface with the existing legacy grant systems in order to ultimately evolve the business processes and concentrate the delivery of the grants mission-set through one major application. SPARTA will interface with the 9 legacy grant systems: (Assisted Firefighter Grant (AFG), Electronic Grants Management System (eGrants), Environmental and Historic Preservation Management Information System (EMIS), Emergency Management Mission Integrated Environment (EMMIE), Grants Reporting Tool (GRT), Hazard Mitigation Grant Program (HMGP), Individual Assistance (IA), Non-Disaster Grants (ND-Grants), and National Emergency Management Information System Public Assistance (NEMIS PA). Additional interfaces include, GMM -  Data Staging Platform (GMM-DSP), as well as the FEMA Applicant Case Tracker (FACTRAX). |
| FEMA - Integrated Public Alert & Warning System (IPAWS) (P) | National Public Warning System | The NPWS is designed for use by the President and other national, state, and local officials to reach the public promptly with emergency information preceding, during, and following an enemy attack or other disaster where the survival of the nation is threatened. |
| FEMA - Logistics Supply Chain Management System (LSCMS) (P) | Logistics Supply Chain Management System Cloud | LSCMS-C provides capabilities for Order Fulfillment, Inventory Management, Transportation, Delivery, and Acceptance of assets and commodities.  LSCMS-C tracks and reports the location of assets and commodities for real time management. The LSCMS-C operational system maintains and manages the inventory at all FEMA Distribution Centers (DCs). |
| FEMA - PIVOT (P) | Pivot-FEMA | The Pivot program is a business system for the National Flood Insurance Program (NFIP) that include insurance policy/underwriting, claims processing, and flood zone mapping. Pivot stores all claims, activities, and documents related to a specific NFIP policy. |

| | | |
|---|---|---|
| FEMA - Risk Mapping, Analysis and Planning IT (Risk MAP IT) (P) | Risk Analysis and Management | The Risk and Analysis Management (RAM) System supports the National Flood Insurance Program (NFIP) and provides an online method to reference and update the maps which define flood plains throughout the U.S. and its territories. FIMA Risk Management Directorate (RMD) provides high-quality flood maps, information, and tools to better assess flood risk, and provides planning and outreach support to communities to help them take action to reduce or mitigate this risk. RMD will operate the RAM. The RAM will support the identification of hazards, assess vulnerabilities, and develop strategies to manage the risks associated with natural hazards. The RAM system supports the following RMD functions: 1) risk-based hazard mitigation planning; and 2) public map and data distribution and customer service. RAM provides support for the development, interaction, or administration of internal and external facing flood mapping services, web applications, the distribution of flood map products, and customer support for FIMA stakeholders and the general public. This supports the FEMA FIMA's mission to mitigate the risk of loss of life and property by providing access to flood mapping products to the Federal, States, and Municipal governments and FEMA contractors at no charge.RAM is the product of the consolidation of two existing systems - Mapping Information Platform-Data Center 2 and Map Service Center in Allegany Ballistics Laboratory Data Center." |
| **Customs and Border Protection (CBP) Systems** | | |
| CBP - Advance Passenger Information (APIS) (P)/CBP - Passenger Enforcement Systems (PES) (P)/CBP - Primary Application Maintenance (P)/CBP - TECS Modernization (P) | TECS | TECS is the cornerstone of CBP's information management strategy for providing support for federal law enforcement missions. TECS provides controlled access to a large database of law enforcement information which interfaces with other Federal, State, and international law enforcement systems. The TECS vision is to collect quality information and provide flexible and reliable information technology alternatives to enhance customer service and assure effective border security.  TECS provides border inspection, investigative, interdiction, intelligence analysis and integrity tracking support software and communications. TECS provides major automation support for the Interagency Border Inspection System (IBIS) serving as the clearinghouse for law enforcement data.  TECS major functions support passenger processing and investigations. |
| CBP - Advanced Trade Analytics Platform (ATAP) (P) | Advanced Trade Analytics Platform Data Ingestion and Integration | ATAP DII provides a single location for accessing internal and external trade mission data required by the Office of Trade (OT).  By using artificial and machine learning algorithms, the data can be analyzed to make well-informed customized decisions that will allow CBP to assume a more collaborative and proactive enforcement and risk-assessment posture. |

| | | |
|---|---|---|
| CBP - Electronic System for Travel Authorization (ESTA) | Electronic System for Travel Authorization (ESTA) | The Electronic System for Travel Authorization (ESTA) is a web-based system intended to both enhance aviation security and strengthen the Visa Waiver Program (VWP) by screening potential travelers, determining their eligibility for travel, and provide an authorization to travel to the United States in advance of that travel. ESTA is designed to: (1) Provide information about VWP travelers in advance of travel; (2)Provide additional information to Customs and Border Protection (CBP) Officers conducting inspections; (3) Reduce delays associated with vetting at the ports of entry (POEs); (4) Reduce the number of travelers that are not admissible at the border. |
| CBP - Analytical Framework for Intelligence (AFI) | Analytical Framework for Intelligence (AFI) | AFI provides DHS-wide Intel Product dissemination, broad search and Analytics for CBP, ICE and other DHS analysts. |
| . | Electronic Visa Update System (EVUS) | The Electronic Visa Update System (EVUS) is a web-based system that facilitates periodic updates of biographical information by U.S. Visa holders from those countries subject to EVUS requirements (as mandated by the National Security Council and the Department of Homeland Security (DHS). EVUS determines the 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. EVUS is designed to: (1) Provide information about visitors with B1, B2, and B1/B2 U.S. visas in advance of travel; (2) Provide additional information to Customs and Border Protection (CBP) Officers conducting inspections: (3) Reduce delays associated with vetting at the ports of entry (POEs): (4) Reduce the number of travelers that are not admissible at the border. |

| | | |
|---|---|---|
| CBP -Automated Passport Control (APC) and Mobile Passport Control (MPC) | Automated Passport Control (APC) and Mobile Passport Control (MPC) | APC:<br>- 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, voluntary, and does not require pre-registration or membership.<br>- The APC self-serve kiosks allow passengers to submit their customs declaration and biographic/biometric information electronically.<br>- The collected data is vetted via federal enforcement systems; once vetted, 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.<br>- 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 reduce processing time roughly in half, which has in turn reduced passenger wait times 20 to 40 percent in locations where APC is available.<br><br>MPC:<br>- Mobile Passport Control (MPC) is the first process utilizing authorized apps to streamline a traveler's arrival into the United States. Eligible travelers voluntarily submit their passport information and answers to inspection-related questions to US Customs and Border Patrol (CBP) via a smartphone (rather than a traditional paper form) prior to inspection.<br>- After passengers 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 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 travelers who successfully use the authorized app will no longer have to complete a paper form or use an APC kiosk. As a result, travelers may experience shorter wait times, less congestion, and more efficient processing. |

| | | |
|---|---|---|
| CBP -Traveler Verification Service (TVS) | Traveler Verification Service (TVS) | The Traveler Verification Service (TVS) is a biometric verification tool developed in response to the federal mandate to biometrically verify and confirm the identity at the time of border crossing for all internationally outbound travelers. Biometric Exit verification is performed through a capture device placed at or near the outbound gate prior to travelers boarding a plane. TVS creates a gallery of traveler photos based on the flight manifest provided by APIS and uses the biographic information to search through various CBP holdings for photos. Upon successful matching, travelers will be confirmed through ADIS and non-USCs will have their encounter photo sent to OBIM/IDENT for enrollment. For unsuccessful matches, TVS will send a notification to CBP Officers who have the option to perform exceptions processing on the traveler. TVS provides a dashboard to view metrics, reports and a visual representation of galleries created for matching. TVS is being used at multiple touchpoints including for Air Entry, Sea Entry, TSA, and Land Pedestrian. Additionally, in support of the "Seamless Traveler Experience", TVS is provided to Airlines to support their Check-In, Baggage Drop, and International Boarding efforts. |
| CBP -Electronic Secured Adjudication Form Environment (e-SAFE) | Electronic Secured Adjudication Form Environment (e-SAFE) | The Electronic Secured Adjudication Forms Environment (e-SAFE) is a Customs and Border Protection (CBP) web-based application, built on the Customer Relations Management (CRM) platform, that serves as the primary public-facing interface for applicants to submit waiver applications directly to the Admissibility Review Office (ARO). |
| CBP - Unified Secondary | Unified Secondary | Provides end to end workflow to process secondary inspections and adverse actions in land, sea and air ports of entry via aircraft, pedestrian, vessel, vehicle, bus and rail conveyances. |
| CBP - Unified Immigration Portal (UIP) | Unified Immigration Portal (UIP) | UIP is a technical solution that connects relevant data from agencies across the immigration lifecycle to enable a more complete understanding of an individual's immigration journey. UIP allows agencies with a role in the immigration system to share agreed-upon information faster and more effectively which establishes connections to mission-critical data and provides insight into interagency operations across the immigration ecosystem. |
| CBP - Air and Marine Operations Surveillance System (AMOSS) (P) | Air and Marine Operations Surveillance System | AMOSS provides the most comprehensive aviation surveillance picture in the Western Hemisphere and promotes the safety and security of the United States and its assets. The AMOC is an active participant in Information Sharing and is the sole provider of critical air and maritime domain awareness data to over 15 DOD partners, 44 DHS partners and 5 other Federal partners. Additionally, AMOSS is utilized during National Special Security Events and SEAR 1 and 2 level events to support specialized airspace security. AMOSS directly supports security efforts beyond the physical borders of the United States. AMOSS is the sole provider of an overarching air surveillance detection fence over and around the Nation which allows the AMOC to coordinate the use of integrated air and marine forces to detect, interdict, and prevents acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward, across, or within the borders of the United States. |

| | | |
|---|---|---|
| CBP - Arrival and Departure Information System (ADIS) (P) | Arrival & Departure Information System | ADIS is a repository of biographic, biometric, and encounter data, consolidated from various systems, on aliens who have applied for entry, entered, or departed from the United States. ADIS is primarily used to facilitate the investigation of subjects of interest who may have violated their immigration status by remaining in the United States beyond their authorized stay. It is also used to assist in determining visa or immigration benefits eligibility and providing information in support of law enforcement, intelligence, and national security investigations. |
| CBP - Automated Commercial Environment (ACE) (P) | Automated Commercial Environment | The Automated Commercial Environment (ACE) is an information technology system which was developed to provide resources to U.S. Customs and Border Protection (CBP), the Trade, and Participating Government Agencies (PGAs). ACE is a multi-year modernization effort supporting greater efficiencies in the import and export of goods, trade compliance, as well as accessing organized trade data and ensuring border security. |
| CBP - Automated Commercial Environment (ACE) (P) | ACE Cloud-CACE | ACE Cloud-CACE (ACE Cloud) provides the cloud environment for the Automated Commercial Environment (ACE) selected application services processing. ACE Cloud is implemented using the CBP Amazon Web Services (AWS) Cloud East (CACE) environment that supports IaaS, PaaS, and a few SaaS services that is FedRamp accredited at the Moderate level. |
| CBP - Automated Targeting System (ATS) Maintenance (P) | Automated Targeting System | Automated Targeting System is a rule-based expert system, developed by CBP's OFO and OIT, that assists in identifying imports which pose a high risk of containing narcotics or other contraband. ATS standardizes, evaluates and scores data received from ACS through the use of over 300 weighted rules derived from targeting methods utilized by Customs personnel. ATS applies artificial intelligence techniques to rank shipments as prospects for further review by Customs inspectors. This system increases the effectiveness of U.S. Customs inspectors of imported cargo by improving the accuracy of the inspector targeting for narcotics and commercial fraud violations. The approach is to process all available data pertaining to entries and manifests against rules, profiles and neural nets in order to make a rapid automated assessment of the risk of each import. |
| CBP - Automated Targeting System (ATS) Maintenance (P) | Automated Targeting System Cloud | ATS Cloud is the cloud-based collection of functionalities and data that have migrated from the existing on-premises Automated Targeting System (ATS). Portions of the existing on-premises Automated Targeting System (ATS) will migrate to a cloud environment in the coming months and years. |

| | | |
|---|---|---|
| CBP - Autonomous Surveillance Towers (P)/CBP - Integrated Surveillance Towers (IST) (P) | Autonomous Surveillance Towers | The CBP AST system is a reliable, scalable, cost effective, re-locatable, short and mid-range tower surveillance capability. It uses Artificial Intelligence (AI) to autonomously detect, track, and identify items of interest (IoI) with no human intervention until the classification stage. This drastically reduces the mental workload and the sensor/operator ratio as compared to other analogous surveillance systems. The system operates with 100% renewable/off grid power, and uses multi-modal communications (ex. Mobile Ad Hoc Network [MANET]) and commercial cellular to ensure that the system is able to function nearly anywhere, to include locations with zero infrastructure. As a rapidly relocatable capability, CBP AST will have the capacity to adapt to shifting threat patterns to support medium and short-range surveillance operations and monitoring of illicit activity. |
| CBP - Biometric Entry-Exit (P) | CBP Amazon Web Services Cloud East | In meeting the Office of Management and Budget (OMB) 2010 Cloud First policy, CBP has established the Office of Information and Technology (OIT) datacenter migration plan. This plan outlines not only the datacenter migration effort, but also the modernization of the legacy applications and systems to re-architect for the Cloud. In line with the OBM's 2010 Cloud First policy, DHS/CBP has chosen Amazon Web Services (AWS) as its cloud service provider. Specifically, the AWS U.S. East/West Region (N. Virginia), Infrastructure as a Service (IaaS) cloud provides a broad set of infrastructure services, such as computing power, storage options, networking and databases, delivered as a utility on-demand, available in seconds, with pay-as-you-go pricing.The stated goal of the OIT Data Center Migration Plan is to reduce the reliance and cost associated with traditional on-premise infrastructure and increase application deployment time. This can be accomplished by leveraging the AWS IaaS cloud native services, and utilizing virtualization and automated provisioning technologies to develop a DEV/SAT/PROD/ADMIN platform and environment that will enable the rapid deployment and provisioning of DHS/CBP applications and systems. |
| CBP - Border Enforcement Coordination Network (BECN) (P) | Border Enforcement Coordination Network | BECN is a suite of IT systems, equipment, and services that support the planning, detection, classification, and analysis of illegal border activity. BECN is currently comprised of the following systems: BPETS BPERT GIS ORBBP E3 ICAD TAK UGS TSM MPC eGIS SDI BECN is the suite of IT systems and services that will enhance existing BEMSD Border Patrol Enforcement Systems capabilities. BECN will provide greater situational awareness, improved process integration and improved information sharing. |

| | | |
|---|---|---|
| CBP - Border Patrol Enforcement Systems (BPES) (P) | E3 | E3 is the next generation of Enforce and WebIDENT.  It is a CBP developed transactional enforcement application that will capture all enforcement actions for Border Patrol agent and CBP officers.  E3 replaces the user interface to the ICE ENFORCE Apprehension Booking Module (EABM) and the incident processing functionality within the Seized Currency and Asset Tracking System (SEACATS). This allows a single-entry system for CBP's Border Patrol agents, CBP Officers, and the ICE agents with regards to enforcement incidents. E3 will reduce the current time of recording adverse action information by CBP officers with a higher threshold of quality of the information recorded as well as reduce/eliminate duplicate data entry. E3 will help facilitate the prosecution and tracking of alien smugglers and human traffickers that operate in our border communities. Additionally, by recording important information it will help maintain continuity within the case and will aid in future U.S. Alien Smuggling cases. Furthermore, it will increase the prosecution of dangerous alien smugglers and human traffickers on both sides of the border that operate with impunity and that endanger the lives of migrants along the border. The information collected will be a valuable asset to law enforcement agencies and will enhance the national security of each government. |
| CBP - Border Patrol Enforcement Systems (BPES) (P) | Intelligent Computer Assisted Detection | ICAD is an alarm and dispatch support system with facilities for accessing national law enforcement databases that support intrusion-detection and agent-dispatching functions of U.S. Border Patrol. ICAD is a highly critical application operating in real-time and is used 24x7. Underground sensors installed along the U.S. border detect various types of activity and relay that information to the receiver/decoder located at Sector headquarters. ICAD interprets sensor information and displays it on an ICAD workstation. ICAD III includes a map display of sensor alarms in near real time. A Law Enforcement Communications Assistant (LECA) reviews this information as it comes online. ICAD systems are uniquely configured for each Border Patrol sector. ICAD data from an individual sector is isolated from remaining sectors. Due to the real-time nature of the information, each individual Border Patrol sector exclusively processes, distributes, and stores ICAD data for that specific sector. |

| | | |
|---|---|---|
| CBP - Border Patrol Enforcement Systems (BPES) (P) | Enterprise Geospatial Information Services | The main objective of the Enterprise Geospatial Information System (eGIS) is to display spatially-enabled data to identify patterns and trends, and to perform associated predictive analysis. Providing exact location information via geographic coordinates stored within the database will allow vulnerability assessments to be made, and corrective action be taken regarding border monitoring. eGIS currently supports nearly every aspect of Border Patrol operations with cartography and analysis. More than 17 Sector and Headquarter elements utilize high-end eGIS desktop applications to monitor and track resource deployment, apprehensions, seizures, deaths, rescues and operational strategies. eGIS has also been used to support Congressional testimony related to border issues as well as federal prosecutions. The eGIS Program will take Border Patrol geospatial capabilities to the next level by providing critically needed capabilities and data over the existing CBP network as services so that they are available to all Agents, all of the time. Geospatial data and services are made available to CBP or Border Patrol application through an integrated service or by a system user going to the eGIS web portal to invoke an eGIS service. A user can select and display high resolution geospatial data (map or imagery) over an area of interest and obtain the precise location of an apprehension or seizure using a location point selector (LPS) service.  The LPS service stores the precise location in decimal degrees in accordance with system requirements for storing data. The eGIS service allows the conversion of coordinates between decimal degrees, latitude/longitude, Military Grid Referencing System (MGRS), and Universal Transverse Mercator (UTM). The selected location can be plotted and displayed on a map or image.  A user can query geospatial data and the precise location of the apprehension or seizure in numerous ways such as time-range, date-range, location, Sector, Station and zone. The selected results can be displayed on a map or image or printed to a hardcopy map.  The map or image can be manipulated by: zoom in, zoom out, zoom to extent, zoom to scale, and pan tools. |
| CBP - Border Patrol Enforcement Systems (BPES) (P) | Shared Situational Awareness Team Awareness Kit | Shared Situational Awareness (SSA) provide CBP officers and agents in the field with increased tactical situational awareness and the ability to share location and other information among small teams, stations, sectors or across other state and federal agencies. SSA is a government-owned smart phone application similar to the Apple Find My Friends application and the Google Trusted Friends application. The app allows trusted team members to share data ranging from location and status of friendly forces and assets, threat data location and disposition, and relevant terrain and environmental attributes in near real time. In addition, CBP may use data derived from the SSA application to measure agent response times to sensor alarms and rescues. |

| | | |
|---|---|---|
| CBP - Border Patrol Enforcement Systems (BPES) (P) | Enterprise Geospatial Information Services Cloud | The main objective of the Enterprise Geospatial Information System Cloud (eGIS Cloud) is to display spatially-enabled data to identify patterns and trends, and to perform associated predictive analysis. Providing exact location information via geographic coordinates stored within the database will allow vulnerability assessments to be made, and corrective action be taken regarding border monitoring. The priority mission of the Border Patrol is preventing terrorists and terrorist weapons, including weapons of mass destruction, from entering the United States. The eGIS Cloud Program will take Border Patrol geospatial capabilities to the next level by providing critically needed capabilities and data over the existing CBP network as services so that they are available to all Agents, all of the time.<br><br>Geospatial data and services are made available to CBP or Border Patrol application through an integrated service or by a system user going to the eGIS web portal to invoke an eGIS Cloud service. A user can select and display high resolution geospatial data (map or imagery) over an area of interest and obtain the precise location of an apprehension or seizure using a location point selector (LPS) service. The LPS service stores the precise location in decimal degrees in accordance with system requirements for storing data. The eGIS Cloud service allows the conversion of coordinates between decimal degrees, latitude/longitude, Military Grid Referencing System (MGRS), and Universal Transverse Mercator (UTM). The selected location can be plotted and displayed on a map or image. A user can query geospatial data and the precise location of the apprehension or seizure in numerous ways such as time-range, date-range, location, Sector, Station and zone. The selected results can be displayed on a map or image or printed to a hardcopy map. The map or image can be manipulated by: zoom in, zoom out, zoom to extent, zoom to scale, and pan. |
| CBP - Border Security Deployment Program (BSDP) (P) | Centralized Area Video Surveillance System | The Border Security Deployment Program's (BSDP) Centralized Area Video Surveillance System (CAVSS) offers CBP a mission critical 24/7/365, fully secure, enterprise-wide, surveillance system that provides an integrated surveillance and remote monitoring capability at all U.S. land Ports of Entry (POEs), select U.S. Border Patrol (USBP) locations, and select airports and seaports. The BSDP: (1)Improves the safety and security of CBP Officers, the traveling public and government facilities: (2) Promotes officer integrity and supports judicial investigations through court admissible video and audio recordings. As the enterprise-wide solution for fixed facilities, also supports the Office of Professional Responsibility (OPR), Office of Intelligence (OI), Air and Marine Office (AMO), Enterprise Services, Operations Support, and CBP Watch. |

| | | |
|---|---|---|
| CBP - Common Operating Picture (P) | Common Operating Picture | Initially, COP system will display still images, video imagery and sensor alerts that have been collected by existing border surveillance systems, specifically, the Integrated Fixed Towers (IFT) and the Remote Video Surveillance System (RVSS). Once fully implemented, the COP-IS will also display data from other border surveillance capabilities being piloted by USBP including: flying surveillance capabilities (e.g., SUAS, TAS), Innovative Towers, subterranean sensors and mobile surveillance capabilities. The COP will display these still images, video, radar tracks, and motion sensor alerts to USBP agents assigned to the C2CEN and USBP agents operating in the field, in real-time for analysis and in support of interdiction response activities. Sharing of CBP border surveillance data to the COP will be implemented in a phased approach. Initial tests will be focused on receiving and displaying still images, video imagery and sensor alerts from the IFT and the RVSS border surveillance systems and sending command information to the tower-based sensors (example: commands to pan, tilt, focus, or zoom the cameras) to support Items of Interest (IoI) investigation activities. As the COP system matures, machine learning and other automated recognition, analysis and identification capabilities will be implemented in the COP system to speed up the IoI investigation process and support faster response activities. Eventually, the COP will serve as a single, unified display platform to support all IoI investigation and response activities for all USBP implemented sensor types. Border surveillance systems providing sensor inputs to the COP solution will continue to provide information to other CBP systems (e.g., the e3 Tracking, Sign-cutting, and Modeling (TSM) tool) as well as USBP-issued electronic devices used by response personnel in the field. |

| | | |
|---|---|---|
| CBP - Cornerstone (P) | Cornerstone | The Office of Professional Responsibility (OPR), Personnel Security Division (PSD), created the Cornerstone information management system to automate and manage the background investigation (BI) process for CBP employees, contractors, and applicants. Cornerstone facilitates the BI process by retrieving, compiling, and distributing information between several information systems during the BI process.<br><br>In support of the CBP law enforcement and national security missions, the OPR PSD conducts background investigations on CBP applicants and employees (both federal and contractor) to determine their:<br>- Initial suitability/fitness for employment with CBP<br>- Continued suitability/fitness for employment with CBP<br>- Eligibility to occupy a national security position or access classified information<br>- Eligibility for access to federal facilities and/or information technology systems<br><br>The level of investigation required is determined by the sensitivity designation of the position applied for or occupied. This designation is established in accordance with Office of Personnel Management (OPM) guidance. OPM has delegated the authority to conduct BIs to CBP. DHS has delegated the authority to CBP to make determinations as to an individual's suitability for employment or eligibility for access to classified information. CBP developed Cornerstone to facilitate a paperless BI process. Cornerstone retrieves, parses, compiles, packages, transmits, and attaches a variety of CBP applicant and employee information and documents. |
| CBP - Counter Measure Unmanned Aerial System (CUAS) (P) | Counter-Unmanned Aircraft Systems | Counter-Unmanned Aircraft Systems (C-UAS) technologies have the capability to mitigate small unmanned aircraft systems (sUAS) threats, which may also have associated capabilities such as detect, identify, classify, and track UAS. CBP has an operational need for rapidly deployable; mobile and agent-portable; and fixed assets to provide situational awareness for CBP personnel in the field, as current surveillance capabilities lack the ability to adequately address sUAS threats. |
| CBP - Customs - Trade Partnership Against Terrorism (C-TPAT) (P) | Customs-Trade Partnership Against Terrorism | Office integration product developed for Customs-Trade Partnership Against Terrorism (C-TPAT) group, that collects information for CT-PAT applicants and allows for on-site review. Customs encourages all importers to become members of C-TPAT. C-TPAT membership involves a process in which the importer documents and performs a self-assessment of the entire supply chain. |

| | | |
|---|---|---|
| CBP - Data Center and Cloud (P) | CBP Mainframe Cloud | In meeting the Office of Management and Budget (OMB) 2010 Cloud First policy, CBP established the Office of Information and Technology (OIT) datacenter migration plan. This plan outlines not only the datacenter migration effort, but also the modernization of the legacy applications and systems to re-architect for the Cloud. In line with the OBM's 2010 Cloud First policy, DHS/CBP has chosen to migrate the CBO IBM Mainframe to IBM Smart Cloud for Government. Systems that are not modernized yet will be modernized yet will be migrated as is to the IBM Cloud solution until such a time that they can be modernized. We are calling our version CBP Mainframe Cloud (CMC). |
| CBP - Data Center and Cloud (P) | CBP Cloud Computing Environment | C3E is a General Support System (GSS) that provides infrastructure and platforms to support numerous CBP applications. C3E includes physical servers and an on-premise cloud which is comprised of virtual machines that act as servers and databases, as well infrastructure that supports the physical and virtual servers and databases. |
| CBP - Data Center and Cloud (P) | CBP Directory Services | CBP Directory Services (CDS) is a general support system (GSS) that provides Windows-based active directory that allows CBP employees/users (using PIV cards) to authenticate and/to log into the CBP Domain and access their files, email, and other CBP applications. The network authentication mechanism allows users, computers, and applications to connect to the network in a common security framework. The system also provides a common electronic-messaging and collaboration environment serving the needs of the enterprise and inter-component communications within CBP. |
| CBP - Data Center and Cloud (P) | Automated Commercial System Mainframe Cloud Application | Tracks trade related information to manage entry and entry summary details pertaining to the assessment, collection, and liquidation of duties, fees, penalties, and taxes owed by trade importers to the Federal Government. |
| CBP - Data Center and Cloud (P) | NDC Data Center Infrastructure | NDC Data Center Infrastructure is designed to provide an application infrastructure on a reliable and secure network platform with high performance connectivity. It is intended for high density installation of commodity and virtualized servers. The infrastructure supports a promote-to-production practice where applications migrate through separate physical environments for development, testing and production. |
| CBP - Electronic System for Travel Authorization (ESTA) (P)/CBP - Global Enrollment Program (P) | e-Business | The Passenger Systems Program Directorate, as directed by the CBP Authorizing Official (AO), has consolidated a number of web-based systems into a single Security Authorization Package (SAP) package named e-Business. The e-Business systems goals are to enhance travel convenience and collect receipts for increased service while impeding the abuse of the privileges. The e-Business systems SAP provides an overview of the security requirements which include the following subsystems: Combined Automated Operations System (CAOS), Decal and Transponder Online Procurement System (DTOPS), and an online reference tool named Terms, Acronyms and Definitions (TAD).The following section provides a general description of the PSPD e-Business systems and identifies the purpose of the system along with its capabilities, users, and information data flow; and discusses the hardware, software and firmware implemented in support of e-Business. |

| | | |
|---|---|---|
| CBP - End User (P) | Field Systems Environment | The Field Systems Environment (FSE) is a CBP General Support System (GSS) that primarily encompasses physical security for the IT infrastructure LAN Controlled Spaces (LCS) of rooms, closets and cabinets that host and secure IT hardware and wiring equipment within the 2523 CONUS and OCONUS locations. CBP locations are broken down within seven (7) Geographical Regions. Sub-systems within FSE are the fleet of print devices and Model Ports Digital signage. Model Ports Digital signage are large monitors placed conspicuously within 20 international airports and Ports of Entry of large cities that provide specially enhanced videos, in various languages, to communicate the entry process while also introducing visitors to American culture. Printer Logic is an Enterprise-wide system that is available on all workstations and provides a convenient, streamlined and simplistic approach for the general User to locate and install networked printers within their geographical area. |
| CBP - End User (P) | CBP Configuration Manager | The CBP Configuration Manager (CCM) manages the deployment, updating, configuring, tracking and accounting of the CBP Authorized Desktop Build (ADB). CCM employs Microsoft Endpoint Configuration Manager (MECM) to push authorized Windows desktop images, updates, and approved desktop software to more than 88,000 endpoints at more than 1080 field sites where CBP operates. Besides software deployment and management, CCM also offers real-time reporting to facilitate troubleshooting, compliance and accounting. CCM is not a financial system and is not considered mission essential. |
| CBP - Financial/Mixed Systems (P) | National Finance Center System | The NFC Local Area Network serves over 500 staff at the Financial Management Services Center located in Indianapolis, Indiana. It provides file and print services locally as well as limited specialized data resources for assembling financial reports. It also provides connectivity to the Customs and Border Protection Wide Area Network and through that access to mainframe, CBP Intranet, and Internet resources. |
| CBP - Global Enrollment Program (P)/CBP - Passenger Enforcement Systems (PES) (P) | Global Enrollment Programs | The purpose of the Global Enrollment Programs (GEP) Security Authorization Package is to document the security in place for Passenger Systems Program Office (PSPO) applications and/or subsystems that support CBP Global Enrollment Programs. The applications and/or subsystems are under PSPO management control, and share similarities in mission, function, objectives, operating characteristics and operating environments. The specific applications and/or subsystems covered are Global Enrollment System (GES) including Trusted Traveler, Trusted Worker and Vetting Center Module applications, Global Entry (middleware, kiosks, and Reporting System), Nexus Air interface, and Outlying Area Reporting Stations (OARS). The general purpose of the applications covered within the GEP Security Authorization package is to provide information system processing support for some aspect of a CBP program sponsored by the CBP Office of Field Operations (OFO). CBP is responsible for protecting America s borders through the screening of incoming travelers at official ports of entry, while at the same time facilitating the movement of legitimate trade and travelers. Various CBP programs created and administered by OFO support this CBP mission by providing pre-screening of individuals, expedited processing of pre-screened travelers by United States officials at selected ports of entry, and the screening of incoming travelers through the use of Alternative Inspection Systems (AISs). PSPO within the CBP Office of Information and Technology (OIT) is responsible for the development and maintenance of IT applications to support the business requirements set forth by OFO for their current and new trusted traveler programs. |

| | | |
|---|---|---|
| CBP - Incident Driven Video Recording System (IDVRS) (P) | Incident-Driven Video Recording Systems | The purpose of the IDVRS program is to provide CBP with a capability to record incident-driven video footage. IDVRS includes body-worn cameras (BWC), BWC docking stations, BWC mounting options, software licenses for officer/agent video management system (VMS) access, network infrastructure improvements (e.g., switches, circuits, and cables), and physical storage for BWCs, docking stations, and mounting options. Freedom of Information Act (FOIA) and Small Unmanned Aircraft System (SUAS) will be managed in Axon's FedRAMP Evidence.com Azure Cloud storage environment used by IDVRS. Evidence.com will be the central management environment for FOIA to redact videos requested from the public before sending the response to the FOIA requestor. The CBP FOIA Office will not store videos in Evidence.com, but will redact the videos, download the redacted video file to a CBP workstation, and upload the file to FOIAOnline, the system of record for all FOIA requests. IDVRS will configure its virtual space to segregate FOIA data from that of other systems residing in Evidence.com. The CBP FOIA users will have accounts and access to only the FOIA space for the purpose of uploading, redacting, and removing videos. For SUAS, its videos will be uploaded to the Axon Evidence.com via the Axon Evidence Upload XT desktop application. |
| CBP - Integrated Surveillance Towers (IST) (P) | Integrated Surveillance Towers | In support of the United States Border Patrol (USBP), the Program Management Office Directorate (PMOD) is under the procurement of hardware and services for the deployment of the Integraged Surveillance Towers (IST) system. The Integrated Surveillance Towers (IST) system consists of the Northern and Southern Border - Remote Video Surveillance System (RVSS), Integrated Fixed Towers (IFT), Autonomous Surveillance Towers (AST) and any other fixed or relocatable surveillance systems. RVSS is a camera-based systems generally deployed anywhere in urban environments in the immediate vicinity of the border wall to detect illegal border activity within seconds or minutes of crossings. IFT is a radar- and camera-based system to detect illegal border activity minutes to hours after crossings. AST is a radar- and camera-based system deployed relevant geographies to autonomously detect, identify, and track Item of Interests (IoIs). The Integrated Surveillance Towers (IST) with the integrated COP program also provides U.S. Border Patrol (USBP) a single program office interface for all their surveillance tower needs, which includes the consolidation of the current Integrated Fixed Towers (IFT), Remote Video Surveillance System Upgrade (RVSS-U), Northern Border RVSS (NB-RVSS), and Autonomous Surveillance Towers (AST) programs. |
| CBP - Integrated Surveillance Towers (IST) (P)/CBP - Remote Video Surveillance System (RVSS) Upgrade Program (P) | Remote Video Surveillance System Upgrade | The RVSS Upgrade system is the Major Application supporting the Office of Border Patrol by deploying new integrated technology solutions to provide enhanced situational awareness capabilities to CBP border enforcement mission. |

| | | |
|---|---|---|
| CBP - IT Security and Compliance (P) | CBP Security Operations | The purpose of the CBP Security Operations (SO) is to monitor connected information systems 24 hours a day, 7 days a week. Daily operations of the Security Operations involve the handling of IT security incidents, while ensuring their timely identification and resolution. The Security Tools Support personnel do the daily operations and maintenance of tools used by Security Operations analysts, including the intrusion Detection and Prevention systems, Security Information and Events Management (SIEM), Host Intrusion Detection Systems (HIDS), etc. |
| CBP - IT Security and Compliance (P) | CBP Network Tools Package | Tools used to manage the CBP production network. |
| CBP - IT Security and Compliance (P) | Identity, Credential, and Access Management | The CBP Identity, Credential, and Access Management (ICAM) system is a major application that provides a centralized role management access service to system owners to control secure logical access to their resources for the CBP enterprise. When users attempt to access an application via a web interface, ICAM displays the view they are allowed to see based on their assigned roles. It is a web-based application comprised of CyberArk and SailPoint and Red Hat Directory Server Lightweight Directory Access Protocol (LDAP). |
| CBP - Mobile Surveillance Capabilities (MSC)/(MVSS) (P) | Mobile Agent Centric Systems | Secure the United States Border to reduce illicit flows and crimes associated with smuggling between the ports of entry and control illegal crossings and cross-border crime by providing mobile surveillance systems that addresses the following capability gaps: 1) The ability to move surveillance capability based on threat behavior; 2) The ability to operate in remote locations that are not logistically or environmentally conducive to fixed tower infrastructure; and 3) The ability to augment and, if necessary substitute for fixed tower surveillance infrastructure. |
| CBP - Network (P) | Enterprise Core Gateway | General support system for the CBP network. |
| CBP - Non-Intrusive Inspection (NII) Systems Program (P) | Non Intrusive Inspection Systems Program | The Non-Intrusive Inspection (NII) Systems Program supports the interdiction of Weapons of Mass Destruction and Effect (WMD/WME), contraband, and illegal aliens being smuggled across the United States borders, while having a minimal impact on the flow of legitimate commerce. The NII Systems Program is an essential aspect of the Customs and Border Protection (CBP) layered enforcement strategy. The goal is to match the technology and equipment with the conditions and requirements at each inspection point, including domestic ports of entry and border patrol checkpoints, and overseas ports, based upon a scientific analysis of the individual conditions at that location. This synchronization will increase the effectiveness of the strategy by strengthening one of its most vital layers. The purpose of the NII Systems is to enable CBP to perform more effective and efficient non-intrusive inspections and screenings of cars, trucks, railcars, sea containers, personal luggage, packages, parcels, and flat mail. |
| CBP - Non-Intrusive Inspection (NII) Systems Program (P) | Radiation Detection Equipment | Radiation Detection Systems and Equipment (RDE) provide a passive, non-intrusive means to scan cars, trucks and other conveyances for the presence of radioactive and nuclear materials. Customs and Border Protection has deployed a variety of these systems nationwide in an effort to scan 100% of all incoming vehicles and cargo for gamma ray and neutron radiation emanating from natural sources, special nuclear materials and isotopes commonly used in medicine and industry. |

| | | |
|---|---|---|
| CBP - Non-Intrusive Inspection (NII) Systems Program (P) | Non-Intrusive Inspection Integration Program | The mission of the NII-I Program will be the same as the legacy NII Program, however, the NII-Integrated Program will migrate NII operations from a standalone system configuration to a cloud-based integrated architecture. This will allow X-ray images from multiple POEs to be routed to AWS for central adjudication. This will also provide interoperability with other cloud-based CBP applications and data routing to the AWS ARDIS-C for data storage. |
| CBP - Non-Intrusive Inspection (NII) Systems Program (P) | Port Radiation Inspection, Detection & Evaluation | The purpose of the Port Radiation Inspection, Detection and Evaluation System (PRIDE) is to provide nuclear and radiological detection and adjudication for all conveyances and people crossing domestic U.S. Land Border Crossings and shipping containers at U.S. Ports of Entry. PRIDE is based within the continental U.S. borders and was developed as part of the Non-Intrusive Inspection (NII) Program. It interfaces with several NII developed technologies such as the Radiation Portal Monitors (RPM), Radiation Isotope Identification Device (RIID), the Visual Identification System (VIS), and other devices to collect and consolidate data from all such devices at a centralized location and provides a Web Based Graphical User Interface (GUI) and adjudication tool-set that allows Laboratory Scientific Services (LSS) to review the alarms and any additional onsite information from local CBP Officers, allowing them to participate in the adjudication of such alarms in a near real time basis. |
| CBP - Non-Intrusive Inspection (NII) Systems Program (P) | Automated Radiological Data Integration System Cloud | ARDIS-C is the cloud iteration and continuation of operation of the ARDIS legacy system and repository for all Radiation Portal Monitor (RPM) data, X-ray images, and metadata collected at Ports of Entry (POEs) and Ports of Lading (POLs). ARDIS-C receives automatic data delivery by an electronic connection to RPM and X-ray system computers via the U.S. Customs and Border Protection (CBP) PRIDE system and through the Secure Wireless InterFacility Transport (SWIFT). Currently data is also delivered by CD, DVD, and external media handling from POEs and POLs to the Data Analysis Center for threat Evaluation and Reduction (DAC-TER). |
| CBP - SAP (P) | SAP | SAP is an Enterprise Resource Planning (ERP) System providing an integrated, enterprise-wide information software solution. As the financial management system of record for CBP, SAP provides the complete integration of business processes within one system, financial statement reporting and internal controls, data accuracy, single system reporting, and enhanced analytical reporting. It also complies with Federal Government standards and regulations for financial management systems. The CBP SAP solution supports the customer, Office of Finance (OF) business requirements. It provides functionality in five key business areas to fulfill CBP's mission: Finance; Procurement; Budget Execution; Business Analytics and Reporting; and Property and Inventory Management. |

| | | |
|---|---|---|
| CBP - Seized Asset and Case Tracking System (SEACATS) (P) | SEACATS Cloud | SEACATS Cloud is a web-based system with a component hosted in the cloud that provides Custom and Border Protection (CBP) with a single repository for enforcement actions related to the Treasury Forfeiture Fund (TFF), as well as seized property inventory and case processing information related to arrests, seized and forfeited property, fines, penalties, and liquidated damages. SEACATS Cloud is managed and operated by the CBP Office of Field Operations (OFO) for use by the OFO Fines, Penalties, and Forfeitures (FP&F) and the U.S. Border Patrol' Asset Forfeiture (AF) divisions, including use by other departments and agencies with similar law enforcement responsibilities to: (1) provide accurate and timely management information; (2) measure seizure performance; (3) track seized and forfeited property; (4) provide a single, accurate repository for case and incident information; (5) document individuals and businesses who violated, or are alleged to have violated, customs, immigration, agriculture, or other laws and regulations enforced or administered by CBP; (6) collect and maintain records on fines, penalties, and forfeitures; and (7) collect and maintain records of individuals who have provided assistance with respect to identifying or locating individuals who have or are alleged to have violated customs, immigration, agriculture, or other laws and regulations enforced or administered by CBP and its partners. |
| CBP - Tactical Communications (TAC-COM) Modernization (P) | Land-base Mobile Radio | Land-base Mobile Radio (LMR) is the system that provides encrypted mission critical voice communications for CBP. The system is primarily used as a tactical tool to assist U. S. Border Patrol and CBP Air Marine Operations communicate in remote areas and maintain officer safety in the field. The Office of Field Operations CBP Officers use the tactical capability at Ports of Entry across the United States. The system is designed to support interoperability amongst and between DHS Agencies, other Federal Agencies as well as State, Local, Tribal and Territorial responders. The system consists of end user handheld and mobile radio devices, an integrated Internet Protocol (IP) based network of radio repeaters and dispatch consoles, as well as network controllers and a Key Management Facilities (KMF). |
| CBP - Tethered Aerostat Radar System (TARS) (P) | Tethered Aerostat Radar System | Tethered Aerostat Radar System (TARS) is an aerostat-borne, surveillance program. Using the aerostat as a stationary airborne platform for surveillance radar, the system is capable of detecting low altitude aircraft over an extended area. TARS provides detection and monitoring capability along the U.S.-Mexico border, the Straits of Florida, and a portion of the Caribbean in support of the Counter-Drug Program with the Department of Defense. The primary mission of the program is to provide persistent, long range detection and monitoring of low-level air, maritime, and surface narcotics traffickers using radar detection. |
| CBP - Unattended Ground Sensors (UGS) (P) | Unattended Ground Sensors | The USBP UGS program includes a broad range of remotely monitored surveillance systems placed in areas where there is generally no persistent presence of CBP personnel in the immediate vicinity of the device. UGS is an overarching term used to describe unattended ground sensors that include seismic, acoustic, magnetic, and day/night cameras that are used to automatically detect persons or vehicles and transmit activity reports or images via radio frequency, microwave, cellular or satellite communications to the CBP Intelligent Computer Assisted Detection (ICAD) application suite. In addition, trigger or queue large platform surveillance and provide notification of areas requiring USBP agents to respond and resolve. |
| CBP - Unified Immigration Portal (UIP) (P) | Unified Immigration Portal | National Targeting Center Agents and Officers who identify, dismantle, and disrupt illicit networks will use the UIP as an interactive, cloud-based research tool to expedite the research process by illuminating connections across large, disparate data sets. This enhances national security by strengthening CBP's ability to analyze and exploit mission-critical data. |

| | | |
|---|---|---|
| **Federal Law Enforcement Training Center (FLETC) Systems** | | |
| FLETC - Financial Management System (FABS) (P) | Financial Accounting and Budgeting System-FLETC | The FABS application is an all-in-one financial processing system. It functions as the automated accounting and budgeting system for the FLETC. |
| FLETC - Student Administration & Scheduling System (SASS) (P) | Student Administration and Scheduling System | This is a FLETC enterprise-wide system encompassing the majority of the FLETC's mission–critical processes. The system's primary functions include an automated scheduling system, a student registration and management system, a testing and evaluation function, a tuition development and validation component, and a student billing component. |
| **United States Immigration and Customs Enforcement (ICE) Systems** | | |
| ICE -Exodus Accountability Referral System (EARS) | Exodus Accountability Referral System (EARS) | EARS is an intranet-based system developed for ICE and CBP to track and manage the License referral process. To enforce U.S. federal export control laws, ICE and CBP require information from federal regulatory agencies that grant export licenses on controlled items, specifically whether a license is required and whether a license has been granted. The ICE Exodus Command Center operates the Exodus Accountability Referral System, an ICE database that initiates, tracks, and manages requests to regulatory agencies for this information. ICE and CBP obtain relevant information from several other sources, such as business records and publicly available information from the Internet, to develop sufficient knowledge of the pertinent transaction, commodity, business entity or individual. This information is used by the licensing agencies to check against their records to determine if the Principal Party in Interest has the proper license/authorization to conduct the export activity in question. Federal licensing agencies that receive EARS referrals provide information based on their internal records on determinations on the need for licenses and information on licenses and licensing history in response to EARS referrals from ICE. Responses from the licensing agencies are scanned and uploaded into EARS by ICE ECC personnel for review by the requesting ICE agent and/or CBP officer. EARS itself is the source of statistical reports generated by the system. |
| ICE- ICE Analytics | Law Enforcement Information Sharing Service | The purpose of the LEISS system is to provide a conduit for external law enforcement entities (non-ICE, inclusive of local and state law enforcement agencies) to identify suspect identities and discovering non- obvious relationships among individuals and organizations for investigating violations of customs and immigration laws as well as possible terrorist threats and plots. This is accomplished through the custom applications, databases that were acquired and web service developed and deployed to meet the missions needs. |

| | | |
|---|---|---|
| ICE - License Plate Reader | License Plate Reader | License Plate Reader Platform is Project Southern Ground - an ICE HSI-led initiative that uses LPR technology, including data gathered by commercial entities and other law enforcement agencies, to support and further advance transnational criminal investigations (i.e. national security threats, illegal arms exports, financial crimes, and human trafficking). All LPR systems use proprietary software that is vendor-owned and allow HSI Bulk Cash Smuggling Center (BCSC) personnel and designated HSI personnel to upload license plate alert lists, deconflict queries with other law enforcement personnel, and conduct LPR data analytics. The BCSC, where Project Southern Ground is based, currently queries the following systems for information pertaining to the vehicle's location:<br>•Vigilant Solutions, Inc. LEARN LPR database: The Vigilant database collects LPR data from both private and public contributors, including law enforcement agencies, parking garages, and repossession companies. Vigilant makes its LPR data available on a fee-for-service basis to various entities, both public and private. LPR data is stored for immediate or future queries, which may be manual or automatic.<br>•Houston High Intensity Drug Trafficking Area (HIDTA) ELSAG3 LPR system: The Houston HIDTA LPR network consists of participating federal, state, and local law enforcement agencies which operate fixed and mobile cameras in Texas, Kansas, North Carolina, and Georgia.<br>•U.S. Customs and Border Protection (CBP) Unified Passenger System (UPAX): CBP, which owns UPAX, uses LPR devices at and near border crossings and at border patrol checkpoints for law enforcement and safety purposes. LPR data is automatically entered into UPAX, which allows authorized personnel to query the system by license plate number. HSI currently has read-only access to UPAX.<br><br>LPR platforms allow authorized HSI users to create alert lists. Once uploaded to one or all the systems above, alert lists are accessible only by select law enforcement personnel with a need to know. When an entry on an uploaded alert list matches a license plate in an LPR system, HSI receives an automated notification from the system in near real-time. The notification is sent to the designated HSI points of contact that were entered when the alert list was created. Notifications can include an image of the license plate, a computer-generated text of what the software believes is on the plate, and the latitude and longitude of the location at which the license plate was photographed by LPR cameras.  Moreover, HSI can use vendor-owned tools to analyze data collected from LPRs. The vendor-owned analytical tools can determine if plate reads are duplicated within a given time frame and in the same location, helping to identify a pattern of vehicle movement. For example, BCSC personnel may determine the driving patterns of a suspect vehicle along a known smuggling route. Based on the amount of time between LPR camera detections of the vehicle, HSI can determine whether the vehicle made any stops along the route.<br>If investigators later link a license plate to an individual based on separate research in law enforcement databases, this linkage will |
| ICE - OCIO Workstations with File and Print Servers | OCIO Workstations with File and Print Servers | The OCIO Workstations with File & Print Servers (OWFPS) form a general support system (GSS) supporting over 900 ICE field sites across CONUS and OCONUS regions. The functionality of the OWFPS system is to provide workstation, laptop, print services, and file services to all ICE program areas. Print servers allow ICE users to utilize networked printing. The file servers provide a networked file repository for all groups and users. OWFPS architecture reflects all ICE workstations, laptops, file servers, printers, and print servers managed by the ICE OCIO IT Field Operations (ITFO) Branch.  OWFPS workstations and servers are Windows-based operating systems. |

| | | |
|---|---|---|
| ICE - Online Detainee Locator System (ODLS) | Online Detainee Locator System (ODLS) | The Online Detainee Locator System (ODLS) is a publicly accessible, web-based system owned by U.S. Immigration and Customs Enforcement (ICE). ODLS allows the public to conduct online Internet-based queries to locate persons detained by ICE for administrative violations of the Immigration and Nationality Act. ODLS is intended to allow members of the public, especially family members and legal representatives, to determine whether an individual is currently in ICE detention and, if so, at which facility the person is detained. It is a Privacy Sensitive, public facing ICE website that draws its select set of PII detainee information from an EID DataMart. Additionally, it has a unique set of requirements (no user accounts, no authentication, etc.) that permits public access but sets it apart from the functionality of other applications. |
| ICE - OPLA Case Management System | OPLA Case Management System | The OPLA Case Management System (OCMS) is a web-based case and document management system that provides core matter and document management functionality for U.S. Immigration and Customs Enforcement's (ICE) Office of the Principal Legal Advisor (OPLA). OCMS PLAnet is used nationwide by 1,870 ICE OPLA attorneys and over 6,615 HSI and ERO agents to detain and remove priority aliens, and to enhance efficiency in the alien removal process. Through a Web View version, OCMS PLAnet provides law enforcement agents with live Case data that supports mission critical - field level detention and removal activities. With the electronic Service (eService module), OPLA PLAnet has established a Cloud based solution that allows OPLA attorneys nationwide to securely receive and transmit legal communications and documents which contain SPII with the private bar. |
| ICE - VSPTS PATRIOT | VSPTS PATRIOT | The VSPTS project and systems support the work performed by the ICE Visa Security Program (VSP). The mission of the VSP is to provide law enforcement and investigative expertise to the process of vetting individuals applying for visas to enter the U.S., specifically to identify applicants for U.S. visas who are ineligible to enter the U.S. due to criminal history, terrorism associations, or other security-related grounds. The VSP program performs vetting investigations on specific applicants and provides issuance recommendations to the Department of State (DOS). |
| ICE - PLX Cloud Enterprise System (formerly Pen-Link) | PLX Cloud Enterprise System (formerly Pen-Link) | PLX Cloud Enterprise is the law enforcement software package used by the U.S. Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations (HSI) Special Agents, Criminal Research Specialists, and Intelligence Research Specialists for the lawful interception, collection, storage, and analysis of telecommunications records obtained during the course of criminal investigations. PLX Cloud Enterprise is an investigative tool that provides both manual and automated methods of inputting, receiving, maintaining and sharing investigative information with other HSI investigators and analysts, with the goal of providing HSI Special Agents the ability to take disparate information and show organizational links related to a case. This linkage, in turn, helps HSI Special Agents identify relationships that may help to identify the parties of the criminal network under investigation. |

| | | |
|---|---|---|
| ICE - Repository for Analytics in a Virtualized Environment (RAVEn) | Repository for Analytics in a Virtualized Environment (RAVEn) | The Repository for Analytics in a Virtualized Environment (RAVEN) is an ecosystem consisting of industry standard big data tools that enable ICE users in multiple HSI offices and programs to perform analytics across ICE data sets and/or develop new tools to accomplish specific functions. RAVEN tools clean, organize and index data, thereby facilitating analysis to isolate criminal patterns and identify trends and weaknesses in criminal organizations that investigators can use. RAVEN is dedicated to the Dataflow Programing Paradigm (DPP), through which the system is set to identify types of tasks and match them with the tool(s) best suited to accomplish each task. RAVEN chains together existing ICE analytical platforms, enabling users to complete tasks currently considered too large or complex for individual systems. RAVEN Platform generally consists of two large components. A "data lake" i.e., a collection of applications, tools and services designed to efficiently store and process large amounts of different types of data in a variety of formats (e.g., relational and NoSQL databases, files, graphs, images, archives etc.) and a collection of web applications including one mobile application designed to meet the needs of HSI Agents and Analysts that can access the data that resides in the RAVEN data lake. The data lake portion of the platform consists of tools like AWS EC2 and RDS instances, Cassandra, ElasticSearch, NiFi, Kafka and Hortonworks Data Platform (HDP). The application portion of the platform consists of collection of custom Java Spring Boot and React microservices deployed inside Docker containers running in Red Hat OpenShift cluster. RAVEN Team uses ICE provided tools such as Ansible, Jenkins, GitHub, Katello, SCCM, and Splunk to develop, build, configure, deploy, and maintain RAVEN clusters and microservices. |
| ICE - RAVEn Data Analysis & research for Trade Transparency System | RAVEn Data Analysis & research for Trade Transparency System | Data Analysis & Research for Trade Transparency System (DARTTS) is a system that contains trade data between US and foreign partners. The system is available to both US and foreign partners and allows users to see both sides of trade transactions, making them fully transparent to all parties. HSI Trade Transparency Unit (TTU) uses DARTTS to analyze trade data and identify trade transactions and other information that do not appear to follow normal patterns. By seeking out anomalies, HSI Special Agents and Analysts can identify possible criminal activities such as trade-based money laundering (TBML), customs fraud, contraband smuggling, and intellectual property rights violations. |
| ICE - TechOps General Support System (National Tracking Program) | TechOps General Support System (National Tracking Program) | The purpose of the TechOps GSS is to provide basic data networking for disparate systems at the TechOps facility that are not connected to IRMNet. To support TechOps management and operation functions, TechOps uses the GSS to serve as an IT infrastructure, hosting various applications and peripherals used/accessed by management, investigators, and support staff to successfully accomplish their day-to-day activities. The Title III Digital Collection System currently is comprised of 7 physical servers and 45 virtual servers in Lorton, VA that are used to support the interception, recording, and monitoring of oral, wire, and electronic communications, such as telephone conversations and emails, during criminal investigations conducted by ICE and/or other law enforcement agencies. |

| | | |
|---|---|---|
| ICE - Title III Digital Intercept Collection System | Title III Digital Intercept Collection System | Title III Digital Collection System (DCS) is used to support the interception, recording, and monitoring of oral, wire, and electronic communications, such as telephone conversations and emails, during criminal investigations conducted by ICE and/or other law enforcement agencies. These intercepts are commonly referred to as "electronic surveillance" and are always authorized by either a court order (usually federal but in some cases pursuant to a state court order) or the consent of a party to the communications usually a cooperating witness or confidential informant. ICE uses DCS to support its own criminal investigations, criminal investigations conducted by interagency task forces that include ICE, and criminal investigations conducted by other federal agencies. |
| ICE - Criminal Alien Identification Initiatives (CAII) (P) | ACRIME Modernization, LESC | ACRIMe Mod, the Immigration Alien Query (IAQ) processing application, is used to search relevant law enforcement systems to determine immigration status and criminal history. More than 100 Law Enforcement Specialists (LESs) and Officers use ACRIMe Mod to process more than 1.5 million IAQs submitted to the Law Enforcement Support Center (LESC) in Vermont each year. An Immigration Alien Response (IAR) reports the results of the LES research. IARs are transmitted to the original submitting agency and to ACRIMe Field. The receiving Officer manages the IAR active queue in ACRIMe Field ensuring the highest priority IARs take precedence. The Officer can then make a final status determination and begin processes for taking any appropriate enforcement actions. |
| ICE - IT Operational Services (P) | Active Directory Exchange-ICE | ADEX provides ICE and its user community with a common, integrated Active Directory (AD) and Microsoft (MS) Exchange messaging infrastructure, and Enterprise Domain environment. ADEX is a major application that manages all LAN user accounts with standard security group policy settings. Utilizing MS Exchang eserver software to provide email services. The Exchange services include email receipt and transmission, address book, calendar scheduling, and task workf locollaboration tools. |
| ICE - Financial Support Systems (P) | BMIS Web | The U.S. Immigration and Customs Enforcement (ICE) Office of Financial Management (OFM) uses BMIS Web to support the tracking and recording of bond management activities. BMIS Web provides OFM an automated mechanism for maintaining and reporting on all immigration bonds. The agency uses immigration bonds to efficiently administer immigration laws. |

| | | |
|---|---|---|
| ICE - Detention and Removal Operations Modernization (P) | eBonds | The Bonds Online System (eBONDS) is a web-based application used primarily by surety agents and the Office of Enforcement and Removal Operations (ERO) at U.S. Immigration and Customs Enforcement (ICE) to facilitate the ICE immigration bond management process. In June 2010, ICE deployed eBONDS Phase One, which allowed surety agents to post surety bonds electronically for detained aliens determined by ERO to be eligible for release on bond. ICE is now implementing eBONDS Phase Two, which will further automate the bond management process by permitting ICE to send electronic notifications to surety agents within eBONDS, eliminating the current process in which those notifications are sent by U.S. Mail or fax. ICE is also implementing an electronic document repository to store all bond-related documents provided and made available to surety agents via eBONDS. The eBONDS system provides DHS with a means to facilitate bond process data entry by the private sector. The eBONDS system provides the capability for the surety to complete the I-352 Immigration Bond form using web page technology. Once data has been entered into the system, it generates a PDF bond form documentation package, complete with a power of attorney form,I-352, and digital signature capability. A typical system transaction would be for a surety company employee to login to the eBONDS system, request alien bondable status and fill out the on-line I-352 form. Once they submit the form, the system generates the I-352 PDF bond form along with the digital signatures and attaches the current power of attorney form from Bond Management Information System/Web Version (BMIS Web). The PDF bond documentation package is then uploaded to Enforcement Alien Removal Module (EARM) for review and approval by a bond specialist.eBONDS is a secure, public-facing web application that allows surety agents to electronically post surety bonds for the release of aliens in ICE custody. It also provides an electronic, auditable means for ICE to communicate with surety agents regarding active surety bonds. |

| | | |
|---|---|---|
| . | Electronic Health Records | The eHR enables the ICE Health Service Corps (IHSC) to effectively administer and oversee healthcare services delivered to detainees in ICE custody, improve the quality of care delivered, expand the availability of medical information to all providers, reduce duplication of services within the ICE healthcare system, better manage infectious diseases, reduce the medicolegal risks and costs to ICE, implement a standardized approach to healthcare delivery, and leverage community best clinical practices in medicine. The eHR is provided as a Cloud based implementation. The Cloud infrastructure provider is the Azure ICE Cloud. The eHR is comprised of several commercial-off-the-shelf (COTS) software applications that provide electronic medical records and portal, dental health records, pharmacy and medication administration, and medical treatment referrals. eHR is currently comprised of the following components/applications: (1) eClinicalWorks (eCW) her application - a commercial electronic medical records product specifically configured for ICE correctional facility medical services management of healthcare delivered to ICE detainees. This service streamlines the care provided to detainees, automates medical documents, enhances medical management and oversight, and enhances standardization of care provided to detainees. (2) eClinicalWorks Business Objects (eBO) application - a commercial business intelligence reporting application specifically designed for the eCW eHR application and supports overall ICE Health Services Corps (IHSC) management. (3) Open Dental (OD) dental record application - a commercial dental electronic medical records product integrated with the eCW application. (4) Correctional Institution Pharmacy System (CIPS) application - is a centralized, commercial pharmacy application used to manage the distribution of medication within detention facilities. It also allows pharmacists to monitor and track inventory, generates labels for prescriptions that a detainee takes, and checks for drug interactions among all the prescriptions a detainee is taking. (5) Electronic Medication Administration Records (sMARt) application - is a centralized, commercial application used to administer prescribed medications to detainees. The application facilitates the distribution of medications through barcode scanning and provides administration records and reporting. Medical Payment Authorization Request 2 (MedPAR2) application - an upgraded version of the Legacy MedPAR application with direct interfaces to both DHS's ENFORCE Integrated Database (EID) Services and the eCW eHR. |

| | | |
|---|---|---|
| ICE - Detention and Removal Operations Modernization (P) | Electronic Travel Document | : ICE's mission is to protect America and uphold public safety. This is accomplished, in part, by facilitating the removal of aliens who are ordered removed or granted voluntary departure from the United States. eTD was created to provide efficiencies for ICE and foreign governments in filing requests and granting issuance of travel documents. ICE Enforcement and Removal Operations (ERO) are responsible for ensuring that removable aliens in the United States are removed in a timely manner. When an alien is ordered removed from the United States, a consular official from the alien's country of citizenship must issue a travel document if required for entry into his or her country of citizenship or required by a country, which is transited in his or her removal itinerary. This travel document serves as a temporary passport that allows the alien to return to his or her country. Not all foreign governments have elected to fully participate in the eTD process. For "non-participating countries," ICE uses eTD only to create the travel document package and the remainder of the travel document process is handled outside of the eTD system. For "participating countries," both ICE and the foreign government's consular officers use eTD for the full travel document process, i.e., to coordinate the submission, review, and update of the travel document package, as well as the certification or denial of the travel document. The eTD system allows for correspondence to travel between ICE and foreign government officials in the travel document request process via an internet-based system. The eTD system allows foreign consular officers to electronically view travel document requests and issue travel documents from the consulate, eliminating the process of requesting travel documents by mail and ultimately contributing to more expeditious removals. System Functionality: ICE Enforcement and Removal Operations (ERO) are responsible for ensuring that removable aliens in the United States are removed in a timely manner eTD provides an efficient means for ICE personnel to request, and foreign consular officials to review and adjudicate travel document requests for aliens who have been ordered removed or granted voluntary departure from the United States but do not possess valid travel documents. In order to remove foreign nationals who have been ordered removed from the United States, ICE generally needs a valid unexpired passport or other travel document issued by an embassy or consulate to schedule and facilitate the alien's departure from the United States.The eTD system accelerates ERO's process by making travel documents available in an electronic format. The travel documents are electronically generated by ERO or by the field office and uploaded into eTD as a document request package. The package is then forwarded to the consulate. The consular uses eTD to electronically review the travel document request and interviews the detainee to verify citizenship to determine if the request will be issued, held, or denied. If the document is issued, the consular user can sign the document in eTD using a digital signature pad; this also enables ERO users to retrieve and print documents at the detention facility or field office. In addition to the capabilities above, the eTD system builds the contents of a digital travel document request package by pulling information from the Enforcement Integrated Database (EID), such as charging documents, Form I-217 Information for Travel Document or Passport, photographs including fingerprints from the Automated Biometric Identification System (IDENT), and by scanning hard copies of documents such as removal orders, criminal records, forms |

| | | |
|---|---|---|
| ICE - Detention and Removal Operations Modernization (P) | ENFORCE Alien Removal Module | ENFORCE Alien Removal Module(EARM) is an Immigration and Customs Enforcement (ICE) Enforcement and RemovalmOperations (ERO) owned and managed Linux web and database-based removal case mmanagement system, with a host of subsystems and modules, that resides in the AWS ICE Gov Cloud. EARM provides personal identifiers, photographs, and details of removal case proceedings to aid ERO in carrying out the detention of noncitizens and removal of noncitizens from the United States. ICE ERO personnel use EARM primarily as a case management tool to track the status of noncitizens removal proceedings, process removal of illegal noncitizens from the United States cases, and to enter a person's case information. EARM is part of the Enforcement Case Tracking System (ENFORCE), which is a database system that allows ERO agents and officers to identify, book, detain, and track individuals of interest to ICE. EARM interfaces with internal ICE and external DHS enforcement systems to support alien removals, detentions, and alternatives to detention program activities. Internally, EARM interconnects with ICE ENFORCE Integrated Database (EID), Bond Management Information System Web (BMIS Web), Electronic Bonding System (eBONDS), Alien Criminal Response Information Management System, Modernization (ACRIME), and electronic Travel Documents (eTD). EARM pulls data from the subject's record via ENFORCE Integrated Database (EID) that was entered in the ENFORCE. EARM has an external interconnection with the U.S. Department of Justice Executive Office for Immigration Review (EOIR) Justice Consolidated Office Network (JCON)/eWorld General Support System (GSS) Global Web Service Environment (GWSE) for the express purpose of exchanging immigration case and scheduling data between the ICE EARM application owned and operated by ICE, and the EOIR GWSE owned and operated by DOJ EOIR. EARM also interconnects with USCIS, which contains information on the status of 58 million individuals, including permanent residents, naturalized citizens, border crossers, apprehended aliens, legalization aliens, aliens issued employment authorization, and other individuals of interest to DHS. EARM sends data on aliens in removal proceedings and update CIS with the outcome. |
| ICE - Tactical Communications (P) | P25 Land Mobile Radio Network | The ICE TACCOM mission is to provide tactical communications supporting essential frontline operations for criminal alien enforcement, domestic law enforcement, counter terrorism, and first responder operations with secure APCO1 Project 25 (P25) compliant radio communications. |

| | | |
|---|---|---|
| ICE - Student and Exchange Visitor Information System (SEVIS) (P) | SEVIS Modernization | SEVIS Modernization is a program aimed at the modernization of the current SEVIS Legacy functionalities in support of Student and Exchange Visitor Program (SEVP)'s mission. The SEVP mission functions/modules already modernized, contained within SEVP Amazon Web Services (AWS) SEVIS Mod security boundary, and referred to as subsystems include:<br>-Optional Practical Training (OPT) Portal allows non-immigrants studying in the United States to gain practical work experience in their field of study, typically off-campus. This portal tracks their employment as allowed by the program.<br>-SEVP Professional I515A Tracking System (SPITS) is used to process and track non-immigrant students and exchange visitors' admission into the United States, especially when they arrive without proper documentation.<br>-SEVIS Admissibility Indicator (AI) provides an initial positive or negative admissibility indicator to Customs and Border Protection (CBP) officers at Ports of Entry (POE).<br>-SEVP Data Visualization Dashboard (SEVP I-DVD) is an interactive data visualization tool that focuses on business intelligence. It builds compressive calculations, from existing data, to provide statistical summaries. SEVP I-DVD provides capabilities to explore and analyze relational databases, cloud databases and spreadsheets through querying to generate a multitude of graph types. It offers SEVP users with the ability to spot trends, identity opportunities and make data-driven decision.<br>-The Student Exchange Visitor Program (SEVP) External Training Application (SETA) is a component of the SEVIS Modernization effort for both SEVP and Department of State (DOS). It is an Immigration and Customs Enforcement (ICE) application.<br>-SEVIS Information Sharing (SEVIS Info Sharing) is designed to modernize the existing SEVIS Services and Legacy interfaces as part of the SEVIS Modernization effort. SEVIS Info Sharing is the result of the migration of all the legacy SEVIS interfaces from a Java based architecture into a modern COTS based Enterprise Service Bus (ESB) which allows integrations to other applications within SEVIS. |

| | | |
|---|---|---|
| ICE - Enforcement Systems Data (ESD) (P) | Enforcement Integrated Database | The Enforcement Integrated Database is DHS's common database repository for information concerning the arrest and or encounter of subjects by DHS personnel. EID connects to several databases and applications internal and external to ICE/DHS, and is currently being used by several federal agencies for various law enforcement activities. The system is the comprehensive repository of all records created, updated, and accessed by a number of software applications collectively referred to as the "ENFORCE" applications. The system databases and the ENFORCE applications capture and maintain information related to the investigation, arrest, booking, detention, and removal of persons encountered during two (2) groups of government agencies: ICE - immigration and law enforcement investigations and operations and U.S. Customs and Border Protection's (CBP) Office of Border Patrol and Office of Field Operations. The system creates an event-based record for each encounter conducted by law enforcement officers within these agencies. The system provides users with capabilities to access a person-centric view of the collected data as well through accessing data within the ENFORCE applications. |
| ICE - Consolidated ICE Financial Solution (CIFS) (P) | Robotics Process Automation | Robotics Process Automation (RPA) is a software-based approach to process automation through scripted interactions with existing applications and processes. RPA is most often implemented through third-party software offerings, which allow the development and execution of automations. RPA solutions can work within an existing IT landscape and can be used to automate a wide range of computational transaction-based processes. RPA allows for the execution of automations through pre-determined schedules based on business needs/processes. This allows for flexibility and efficiency as automations are executed as designed without the need for human interaction during runtime. The automations that are created through RPA are programmed to mimic and replicate the actions of a human worker interacting with the user interface (e.g., clicks and interactions that would be visible on a desktop screen). Automations can be programmed to complete tasks that are repetitive, have multiple steps and interact with multiple applications, all within a controlled and centralized system and framework. |
| ICE - ICE Analytics (P) | FALCON | Falcon was designed to identify, apprehend, and prosecute individuals who violate criminal and administrative laws enforced by ICE. The Falcon program augments ICE's ability to review and develop information about persons, organizations, events, and locations by ingesting and creating an index of the data from other existing operational government data systems and providing ICE agents, criminal research specialists, and intelligence analysts with applications that visualize the data to help identify relationships. Falcon supports the investigative work of ICE Homeland Security Investigations (HSI) agents and criminal research specialists by allowing them to search, review, upload, and analyze data pertinent to an investigative lead or an ongoing case. |

| | | |
|---|---|---|
| ICE - Federal Financial Management System (FFMS) (P) | Federal Financial Management System | FFMS is a Chief Financial Officer (CFO) designated financial system and certified software application that conforms to OMB Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS provides the capability to carry out the following basic financial management processes and functions in accordance with the requirements of the Joint Financial Management Improvement Program (JFMIP) certification and the General Services Administration (GSA) Mandatory Federal Supply Schedules. |
| ICE - TECS Modernization (P) | Homeland Security Investigations Data Warehouse | ICE developed the Homeland Security Investigations (HSI) Data Warehouse (HDW) to support its mission to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. |
| ICE - LESIM Systems Enforcement (P) | HSI Net | HSI Net promotes an efficient means of managing, sharing, storing, collaborating, searching, and reporting on HSI information while recognizing the need for appropriate privacy and security controls. HSI Net is available to all HSI personnel for the development of customized, program-specific SharePoint collaboration sites that improve office efficiency and exchange of information.HSI Net features include, but are not limited to: automated workflows, document management, records management (i.e., archival of site data), forms management (i.e., the use of InfoPath forms or forms within the collaboration site to collect and display information), search capabilities, reporting capabilities, auditing capabilities, and integration with Microsoft Office products. |
| ICE - Technical Investigations Program Systems (P) | HSI Spectrum Network | The HSI Spectrum Network is a nationwide system used by the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) to collect video evidence from a variety of sources during criminal investigations. This evidence is used by investigators and U.S. Attorneys in the prosecution of immigration and customs violations. The HSI Spectrum Network is a Wide Area Network (WAN) used by the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) to collect video evidence from a variety of sources during criminal investigations. This evidence is used by investigators and U.S. Attorneys in the investigation and prosecution of crimes under HSI's jurisdiction. |
| ICE - IT Operational Services (P) | ICE Cloud Collaboration Software Suite | The ICE Cloud Collaboration Software Suite (CCSS) employs Microsoft Office 365 which is a service on Microsoft Azure; it is a cloud-based productivity tool that combines the familiar MS Office desktop suite with cloud-based versions of Microsoft's next-generation communications and collaboration services that include on-premise products and capabilities used by ICE today, except that E-mail is offered as a cloud-based service. These applications include Office Online, OneDrive cloud storage, Forms, Microsoft Teams, Exchange Online, Stream, Delve, PowerBI, PowerApps, PowerAutomate, Planner, SharePoint Online, EndPoint Manager, Security and Compliance Center, Azure Active Directory, Microsoft Office 365 Admin Center, Microsoft To Do, Microsoft Defender for Cloud Apps, and Microsoft Defender for Identity. |

| | | |
|---|---|---|
| ICE - Application Hosting Infrastructure (P) | ICE Cloud General Support System | The ICE Cloud is a cloud-based General Support System (GSS) that provides FedRAMP approved Cloud services to ICE program areas. It encompasses the infrastructure as well as the management layers of the cloud environments, providing the resources that allow the Agency to deploy and maintain mission-oriented applications. It also allows the ICE OCIO Operation Division, ICE Network Operations Center (NOC) and Security Operations Center (SOC) to effectively manage and monitor the cloud environment. This includes services designed to help developers simplify provisioning and managing infrastructure, deploying application code, automating software release processes, and monitoring application and infrastructure performance. All systems residing on the ICE Cloud must provide separate privacy documentation to ensure proper coverage. ICE Cloud is leveraging the following Cloud Service Provider's FedRAMP Authorizations: Amazon Web Services (AWS) GovCloud Microsoft Azure Government Cloud Microsoft Azure Commercial Cloud ICE currently uses the Microsoft Azure Commercial Cloud environment for information that may be shared to members of the public, which is not a function supported by the AWS GovCloud or Microsoft Azure Government Cloud. The Microsoft Azure Commercial Cloud may be used in the future for internal-facing systems as well. |
| ICE - ICE Telecommunications (P) | ICE Communications over Networks | The purpose of ICE Communications over Networks (ICON) is to provide network connectivity for ICE and its users. The ICE Communications over Networks provides support for all network devices and data communications that employ the infrastructure throughout ICE and 287(g) sites in the Continental United States (CONUS) and outside the Continental United States (OCONUS). The ICE Communications over Networks has been established by the ICE Office of the Chief Information Officer (CIO) to support all CONUS ICE locations and OCONUS. The ICE Communications over Networks (ICON) is a general support system. ICON provides network connectivity for ICE and it's users. |
| ICE - Decision Support Program (P) | ICE Integrated Decision Support System | The ICE Integrated Decision Support (IIDS) system is intended to support decision making activities for users at ICE. The system encompasses a data warehouse optimized for a Business Intelligence (BI) tool set to provide an easy to use interface for users to analyze and report on the data in the data warehouse. The system extracts pertinent encounter, case, incident, documentation information for non-citizens from EID/EARM/BMIS systems and uses enhanced dimensional data model for facilitating easy slicing and dicing for reporting and analysis. |
| ICE - Technical Investigations Program Systems (P) | ICE Team Awareness Kit | TAK Server is a tactical information management system that facilitates information sharing over small to mid-size networks. TAK Server enables users of the Team Awareness Kit (TAK), including ATAK (Android) and winTAK (Windows), to share information in real time across teams. Team Awareness Kit (TAK) supports rapid mission planning and execution with secured connections over commercial infrastructure System Architecture. The current deployments of the ICE and HSI TAK Servers run on the ICE Cloud, specifically within Amazon Web Services (AWS). TAK Server itself is Government off-the-shelf (GOTS) software and requires Java and Postgres to be installed. |

| | | |
|---|---|---|
| ICE - TECS Modernization (P) | Investigative Case Management | Investigative Case Management (ICM) serves as the core law enforcement case management tool for ICE Homeland Security Investigations (HSI) special agents and personnel supporting the HSI mission. HSI uses ICM to conduct transnational criminal investigations to protect the U.S. against threats to national security and bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. HSI investigations cover the smuggling of narcotics, weapons and various types of contraband; financial crime and export enforcement issues; cybercrime; human rights violations; human trafficking and smuggling; and immigration crime. In addition to criminal investigations, HSI also uses ICM to document its activities concerning civil law enforcement, certain background investigations and inspections related to immigration and customs enforcement. HSI special agents and support personnel also use the information to support legal prosecution of criminal and civil investigations. The system is used to document the subjects of interest to ICE (i.e., persons, businesses, vehicles, vessels, aircraft and things) and de-conflict information about these subjects so that each discrete subject has one primary record. |
| ICE - IT Operational Services (P) | OCIO Workstations with File and Print Servers | The OCIO Workstations with File & Print Servers (OWFPS)form a general support system (GSS) supporting over 900 ICE field sites across CONUS and OCONUS regions. The functionality of the OWFPS system is to provide workstation, laptop, print services, and file services to all ICE programs. Print servers allow ICE users to utilize networked printing. The file servers provide a networked file repository for all groups and users. OWFPS architecture reflects all ICE workstations, laptops, file servers, printers, and print servers managed by the ICE OCIO IT Field Operations (ITFO) Branch. OWFPS workstations and servers are Windows-based operating systems. ICE program offices, such as the Office of Human Capital and Enforcement and Removal Operations, are the end users, or customers, who utilize OWFPS equipment and services. |

| | | |
|---|---|---|
| ICE - Office of Professional Responsibility (OPR) Systems (P) | Physical Access Control Systems | PACS mission is to protect U.S. Immigration and Customs Enforcement (ICE) facilities across the United States, the Office of Professional Responsibility (OPR) / Security Division / Physical Security Operations Unit (PSOU) implemented the Enterprise Physical Access Control System (E-PACS). E-PACS operates access control functions at DHS ICE facilities and is comprised of a suite of applications which serve as a mechanism for the management of electronic access points. E-PACS produces automated transactional reports, documenting what activity took place, where and when. E-PACS applications are divided into four areas: A) identification for access; B) visitor management; C) alarm monitoring and intrusion detection. All four applications and processes operate independently at the direction of the E-PACS Administrator. A) Identification - E-PACS requires an individual's PII so it can authorize physical access to DHS facilities. E-PACS sensors read the information on an individual's Personal Identity Verification (PIV) 2 card to verify if the individual is authorized access. B) Visitor Management - Visitors and construction and service contractors Personnel who have not been issued a PIV card must be identified before being granted access. This is accomplished by having the individual provide the information requested on DHS Form 11000-13 "Visitor Process Information." The Personnel enter the information on the form into the E-PACS visitor management function. This information is then used to conduct a search of the National Crime Information Center (NCIC) to determine if there are any criminal records or outstanding arrest warrants for the individual. The results of the NCIC check are entered into E-PACS. If there is no disqualifying information, such as an outstanding arrest warrant, the visitor is cleared for access. Access requests by foreign visitors (non-U.S. citizens and non-Legal Permanent Residents) are processed through the DHS Foreign National Visitor Management System (FNVMS) |
| ICE - Student and Exchange Visitor Information System (SEVIS) (P) | Student and Exchange Visitor Information System | The Student and Exchange Visitor Information System (SEVIS) is a national security tool/law enforcement system that is used to collect, analyze, maintain and share information on all foreign nationals seeking entry into the U.S. as Student and Exchange visitors as well as the schools that enroll them in order to strengthen National Security. To achieve this, SEVIS certifies and monitors over 10,000 academic and vocational institutions that accept foreign student and exchange visitors nationwide and tracks over 1.1 million non-immigrant students and exchange visitors, their dependents and host families, throughout their authorized participation within their designated programs. This information is collected, analyzed and shared with multiple government partners and federal law enforcement agencies (such as the Department of State, components within the DHS (U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, ICE Counter-terrorism and Criminal Exploitation Unit (CTCEU) in order to identify and taking administrative or law enforcement action against A: Foreign nationals who overstay their period of admission or otherwise violate the terms of their visa, immigrant, or non-immigrant status & B: Schools and entities that facilitate the illegal entry or overstay of non-immigrant students and exchange visitors. |

| | | |
|---|---|---|
| ICE - International Affairs Systems (P) | Visa Security Program Tracking System | The VSPTS project and systems support the work performed by the ICE Visa Security Program (VSP). The mission of the VSP is to provide law enforcement and investigative expertise to the process of vetting individuals applying for visas to enter the U.S., specifically to identify applicants for U.S. visas who are ineligible to enter the U.S. due to criminal history, terrorism associations, or other security-related grounds. The VSP program performs vetting investigations on specific applicants and provides issuance recommendations to the Department of State (DOS). VSPTS is a Web-based system providing functionality to support the work performed by ICE and other Department of Homeland Security (DHS) agents related to DHS and law enforcement investigation of visa applicants to provide recommendations to Department of State (DOS) regarding the issuance of visas to the United States. Its primary functions include capturing data related to the activities performed by agents and capturing investigative notes related to the investigation, with the final recommendation provided by DHS. |
| **Transportation Security Administration (TSA) Systems** | | |
| TSA - Data Ctr., Cloud & HPC | Infrastructure Core Services | The TSA Infrastructure Core Services (ICS) GSS, provides core services to the entire TSA user community to include: Common network services, Active Directory (AD), System Center Configuration Manager, Backup and Recovery (BUR), Domain Administration, File and Print Services, Infrastructure Monitoring services/tools, Jumpboxes, BMC Remedy (ticketing system), Antivirus protections, and Storage Area Networks (SANs). |
| TSA - Data Ctr., Cloud & HPC | TSA Azure | The TSA Azure (TAZ) system is a General Support Services (GSS) providing a platform for production and development services to the entire TSA organization. These development and production environments allow TSA to take full advantage of cloud-native services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) capabilities. |
| TSA - Data Ctr., Cloud & HPC | TSA Azure Office 365 | TSA is utilizing the Microsoft Office 365 cloud computing-based Software-as-a-Service (SaaS) solution subscription offering, to securely deliver productivity, collaboration, and end user<br>communication services. The TSA Azure Office 365 (TSAO365) system provides a cloud-based Software as a Service (SaaS) Microsoft Office desktop productivity tools to the entire TSA enterprise workforce in a scalable, highly available, and cost-effective manner. |
| TSA - End User | End User Computing | The purpose of the End User Computing (EUC) Major Application is to provide DHS/TSA employees and contractors with desktops, laptops, network printers, and other End User Computing applications at the various DHS/TSA locations and sponsored sites. |

| | | |
|---|---|---|
| TSA - FAMS Mission Scheduling and Notification System (MSNS) | Mission Scheduler Notification System | The MSNS program and system provides a broad suite of capabilities to TSA LE/FAMS: Facilitates coordination of air marshal availability and communication of mission assignments with FAMS field offices and air marshals. Provides air marshal mission planning capabilities to FAMS Flight Operations personnel at the Freedom Center. Allocates air marshals to flights, in accordance with TSA's risk-based security strategies, FAMS mission requirements, and FAMS quality of life initiatives. Automatically reserves and purchases tens of thousands of airline tickets for air marshals every month. Tracks mission, both flying and ground, execution and facilitates live mission updates in response to a wide variety of emergent conditions. A tool to track and maintain a wide variety of data related to air marshals including ID's, training, equipment issued, etc. as well as a mobile tool to allow personnel to access mission schedules worldwide. The MSNS system operates 24/7 and has a high availability design that enables continuity of operations even during power and communication losses, to not only schedule, but to track Federal Air Marshals around the world. |
| TSA - IT Security & Compliance | Enterprise Analysis System | The Enterprise Analysis System (EAS) is a Privacy Sensitive System that provides the capability to acquire remotely and unobtrusively the digital images of system storage devices, and to perform forensic investigations based on those images. The Emulation Network (EMNET), also part of EAS, will be used to conduct in depth analysis of cyber threats that may arise within TSA systems. EMNET will also provide a mechanism to conduct remote testing using Indicators of Compromise (IOC) that are seen through Cyber Threat and Forensic Analysis. |
| TSA - Network | TSANet | TSA Network (TSANet) is TSA's main General Support System. Due to its geographically-dispersed topology, TSANet is considered a Wide Area Network (WAN) that consist of a Verizon (Primary) and AT&T (secondary) backbone and circuits that is the transport mechanism to provide end user services to the TSA community and LANs at various sites. Overall the TSA Network is a global network that connects over 600 sites and over 54,000 users. The TSA network is highly secured by the use of encrypted tunnels, Cisco ISE port security and network authentication, firewalls, access control lists, NIDS and HIDS. The network is logically separated from other Verizon and AT&T traffic by a separate VRF (virtual routing and forwarder). |
| TSA - Physical Access Control System (PACS) | Field Security Network | Field Security Network (FSN) is TSA's Enterprise Physical Access Control System (E-PACS). FSN incorporates field offices of TSA and allows the ability to centrally manage the physical access to TSA entry points at the various TSA sites. Due to DHS's mandate that each of its components implement a nationwide Physical Access Control System (PACS) for all government-owned and/or controlled facilities, the TSA Office of Security is implementing a nationwide end to end HSPD-12 compliant PACS solution for all of its field offices. |
| TSA - Platform | TSA Operating Platform | The purpose of the TOP is to serve as the foundation for TSA's long-term operational enterprise application infrastructure. The TSA Operating Platform is the technology infrastructure that provides the foundation and/or shared services for mission-critical, operational, and administrative applications.TOP offers platform and software as a service. As a platform and software as a service provider, TSA systems leverage TOP services and software to develop their own "instance" of the software. |

| | | |
|---|---|---|
| TSA - Platform | TSA Salesforce Platform System | The TSA Salesforce Platform System (TSPS) is a General Support System (GSS) hosted on Salesforce's FedRAMP-approved Government Cloud. TSPS is TSA's target Software-as-a-Service (SaaS)/ Platform-as-a-Service (PaaS) platform and a core component of TSA's "Cloud First, SaaS/PaaS First" modernization and digital transformation strategy. Positioned as an enterprise computing platform, TSPS is envisioned to enable TSA users throughout the agency to securely share and reuse data within and between teams, offices, organizations at all levels. TSPS is intended to evolve and scale to include the integration and automation of workflows, operations, and business processes previously disjointed or siloed in legacy, disparate, and disconnected systems and platforms. |
| TSA - Secure Flight | Secure Flight Phase II | The Transportation Security Administration (TSA) mission is to protect the Nation's transportation systems. Passenger prescreening is a TSA function supporting the Department of Homeland Security (DHS) risk-based approach to aviation security.  Aircraft operators transmit passenger information to TSA, which has the responsibility of determining if that passenger information matches information on the government watch list.  Secure Flight Phase II (SF II) conducts passenger watch list matching for 100 percent of covered U.S. aircraft operator and foreign air carrier flights into, out of, over, and within the United States; as well as any flight via a U.S. aircraft operator anywhere in the world to identify individuals who may pose a threat to aviation or national security and designate them for enhanced or expedited screening or prohibition from boarding an aircraft, as appropriate. SF II goals are to:<br>- Identify high-risk passengers for appropriate security measures/actions and low-risk passengers for expedited screening<br>- Prevent individuals on the No Fly List from boarding an aircraft<br>- Identify individuals on the Selectee List for enhanced screening<br>- Minimize misidentification of individuals as potential threats to aviation security<br>- Protect passengers' personal information from unauthorized use and disclosure<br>SF II enables the secure and efficient travel of the vast majority of the traveling public while protecting individuals' privacy. |
| TSA - Security Operations Center (SOC) | Computer Network Defense System | The Computer Network Defense System (CNDS) system is an Enterprise-wide Security Monitoring Operations Center whose purpose is to identify and facilitate the mitigation of threats, vulnerabilities, and risks to the TSA network and connected information systems. |
| TSA - Security Technology Integrated Program (STIP) | Security Technology Integrated Program General Support System | The Security Technology Integrated Program (STIP) is an agency wide system which enables TSA to move their established airport security system to the next generation of capability by connecting the myriad of transportation security equipment (TSE) to one network. STIP will establish a centralized enterprise data management system that will facilitate the exchange of information between TSE located at the nations airports and the people who use, procure and service them. It will support new innovative approaches to exchanging information and servicing the equipment. STIP will assist managers in more effectively administering TSE, deploying personnel, and adapting to changing security needs. Functions that are performed manually today, such as collecting and storing screener performance data, monitoring screening equipment status, and collecting checkpoint throughput and performance data, will be automated through this new system. |

| | | |
|---|---|---|
| TSA - Technology Infrastructure Modernization (TIM) Program | Technology Infrastructure Modernization | The TIM Program provides end-to-end credentialing and endorsement services for populations of workers and travelers seeking access to the nation's critical transportation systems and other infrastructure. These credentialing services include enrollment, security threat assessment (STA) management, vetting, adjudication and redress, credential and endorsement issuance, expiration, and revocation. TIM System's foundational capabilities support the Transportation Worker Identification Credential (TWIC) population and the TSA PreCheck population. |
| TSA - Technology Infrastructure Modernization (TIM) Program | Vetting and Credentialing System | The Vetting and Credentialing System (VCS) is a common Information Technology platform for automating vetting, credentialing, and encounter management functions to produce Security Threat Assessments (STAs), executing operational responses to security threats, and sharing intelligence information with security partners.  Records in VCS present persons applying for or occupying a position of trust (a credential, benefit, or privilege) in over 40 programs and populations. The system processes biographic and biometric data from applicants within the transportation sector including aviation, surface, maritime and national programs including  TSA Pre-Check, Transportation Worker Identification Credential (TWIC),  Alien Flight School Program, Chemical Facility Workers, Hazardous Materials Endorsement, Aviation Workers, FAA certificate holders, airline operators, cargo companies, and TSA employees and contractors. In addition to biographic based terrorism vetting, the system submits biometric and biographic data to partner vetting programs including SAVE, FBI NGI/Rap Back, DHS IDENT and USCIS to perform criminal history, wants and warrants, and legal presence status vetting. |
| **United States Coast Guard (USCG) Systems** | | |
| USCG - CG Logistics Information Management System (CG-LIMS) (P) | CG-LIMS Technical Information Management | The purpose of Coast Guard Logistics Information Management System (CG-LIMS) is to support the Coast Guard logistics transformation and the future enterprise logistics business model. The information managed by CG-LIMS will provide support for the enterprise financial transformation and accountability of Coast Guard investments. CG-LIMS will be a centrally-managed, integrated, enterprise wide logistics information management system that leverages government and industry standards and best practices. By implementing a logistics system capable of supporting improved business processes and organizational structures, the Coast Guard will optimize operational support, reduce costs across the organization, provide real time financial data, and align with DHS enterprise architecture. Specifically, CG-LIMS must provide the capability to support the enterprise asset management functionality for configuration, maintenance, supply chain, property, and technical information across all business lines. It is the single information management system needed to support logistics for all assets, including aircraft, vessels, and shore facilities. |
| USCG - Command Control and Navigation | Ports and Waterways Safety System | The Ports and Waterways Safety System (PAWSS) is a combination of surveillance and communication sensors that supply information to an operational picture of port marine environments. It is the acquisition program to upgrade existing Vessel Traffic Services. |
| **United States Citizenship and Immigration Services (USCIS) Systems** | | |

|  |  |  |
|---|---|---|
| USCIS - Cloud and Data Center SRI (P) | USCIS Enterprise Hosting Services 1 (Rev4) | USCIS EHS1 is the USCIS enclave that supports USCIS Major and Minor Applications. USCIS EHS1 provides the operating system level support, backup level support, database level support, application security level support, and application level contingency planning support to ensure continuity of operations. In addition, USCIS EHS1 will ensure continuity of operations through monitoring and alerting tools to manage the health and security of the infrastructure. |
| USCIS - Digital Innovation and Development (DID) (P) | Digital Innovation & Development - Information Technology | USCIS created DID-IT to host database and web-based application solutions for service centers, local, district, foreign and regional offices. DID-IT's purpose is to provide a centralized and secure production environment to host 508 compliant, System Engineering Life Cycle (SELC) developed minor applications using Agile methodologies consistent with Management Instruction CIS-OIT-003, Office of Information Technology: Aligning Systems Development, Security, and Operations. |
| USCIS - Document Management Division (DMD) (P) | Integrated Card Production System | The USCIS ICPS includes the subsystems of Card Management (CDMT). The purpose of these systems is to collaboratively prepare, manage, and process benefit card order requests from internal and external interfacing systems. The card orders are processed by high-speed customized laser printing equipment. In addition, these systems transmit card production results back to the originating or card requesting system. Currently, ICPS personalizes and distributes the following secure identity cards: the Permanent Resident Card (PRC) ("green card") and the Employment Authorization Document (EAD) ("work permit"). Card orders originate from the CLAIMS 3 LAN or ELIS Major Applications. |
| USCIS - Fraud Detection and National Security (FDNS) (P) | Fraud Detection and National Security Data System | Fraud Detection and National Security Data System (FDNS-DS) is a centralized data system that increases the effectiveness of the United States (U.S.) immigration system in identifying threats to national security, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system. |
| USCIS - Immigration - CLAIMS 3.0 (P) | CLAIMS 3 LAN | CLAIMS 3 LAN provides USCIS with a decentralized, geographically dispersed LAN-based mission support case management system. CLAIMS 3 LAN tracks the receipting of applicant/petitioner remittances and produces notices documenting the remittance. CLAIMS 3 LAN functionality includes adjudication, archiving, card production, case history, case transfer, on-demand reports, electronic file tracking, image capture, production statistics, and status update and electronic ingestion of applicant data captured through Lockbox and producing final notifications (notices and secure identity documents). |

| | | |
|---|---|---|
| USCIS - Information Security (P) | USCIS Enterprise Security System | The purpose of the ESS is to ensure DHS IT resources are secured and available for the Department to achieve its mission and to validate that security policy and controls are followed throughout the Department. The ESS will achieve this requirement by enabling endpoint visibility and enterprise situational awareness of IT resources across the Department. The ESS provides security incident handling, response, and reporting. All security incidents throughout the USCIS enterprise are handled by ESS including remediation efforts and reporting to DHS. The ESS utilizes Splunk, CrowdStrike, and the Vulnerability Assessment Tools (VAT) to fulfill its mission. |
| USCIS - Information Sharing Environment (P) | USCIS Enterprise Service Bus - 2 | The USCIS ESB2 is the foundation infrastructure that hosts and supports USCIS business services and provides the Service Oriented Architecture (SOA) platform for USCIS. The USCIS ESB2 enables real-time information sharing between enterprise applications within USCIS, DHS, external government agencies and trading partners. USCIS ESB2 allows this to be accomplished with little or no modifications to the connected systems, and serves as the primary means for Enterprise Application Integration (EAI) services for USCIS. The USCIS ESB2 primarily consists of a run-time environment to deploy and manage services. |
| USCIS - Infrastructure (Information Technology Field Services) (P) | United States Citizenship and Immigration Services Network | The CISNet General Support System (GSS) is comprised of Local Area Networks (LANs) at USCIS district offices, field offices, service centers and other related USCIS business offices. CISNet provides the network infrastructure, including office data communications, file and print services to all users at all of the USCIS Sites within the United States. CISNet is responsible for the LANs at each of the sites and connecting the users to the ONENet. |
| USCIS - Infrastructure (Information Technology Field Services) (P) | USCIS Outside the Contiguous United States | The purpose of the OCONUS LANs are to provide office data communications, file and print services to approximately 198 OCONUS system users located at 30 OCONUS sites. The LANs provide users with e-mail and Internet access via multiple connections. |
| USCIS - MyUSCIS (P) | MyUSCIS | MyUSCIS is a public facing website that was developed to assist USCIS customers with obtaining answers to routine immigration questions and access to supporting immigration material. MyUSCIS was designed to allow immigration information to be easily and readily available. MyUSCIS will include intelligent searching and decision tree capabilities via the Explore my options |
| USCIS - Network SRI (P) | Enterprise Infrastructure Services 3 | EIS3 is a new GSS designed to consolidate USCIS communication technologies. EIS3 incorporates video teleconference (VTC), video streaming, voice systems, and digital signage. The equipment is located at USCIS facilities throughout the United States. EIS3 incoporates four subsystems: Video Teleconference (VTC), Video Streaming, Voice, and Digital Signage. |

| | | |
|---|---|---|
| USCIS - Transformation (P) | Electronic Immigration System | ELIS was designed to improve the Electronic Immigration System's (ELIS) architecture by simplifying the existing commercially off the Shelf (COTS) based architecture.  The system is central to the USCIS Goals of improving the effectiveness of adjudicative decisions; increasing security; decreasing adjudication time and lead time for applications and petitions; integrating with the Agency's mission essential information systems; decreasing the maintenance burden from legacy systems; reducing the dependency on paper; and increasing the percentage of the Agency's workload that is fully electronic. It has transformed USCIS operations by taking advantage of digital capabilities to streamline operations and to increase adjudicators' efficiency by ensuring all relevant information is available and accurate at the time of adjudication. ELIS also is a part of an ecosystem of information systems that provides advanced capabilities for fraud detection, national security review, and information services. The capabilities will deliver case intake and account management, benefits case processing, electronic document management, and integration with mission essential USCIS systems and services requirements. |
| USCIS - Verification Modernization (VER) (P) | Verification Information System | Verification Information System (VIS) is a nationally accessible database that contains information on limited citizenship, immigration, and employment status information from several Department of Homeland Security (DHS) systems of records. VIS supports three primary functions: (1) Employment eligibility queries by companies Benefit eligibility queries for Federal, State, and Local government agencies (e.g., driver's license, green card, or work permit) (2) Provides USCIS staff the means to support case management of disputed eligibility queries and to identify/track fraudulent behavior associated with eligibility queries. (3)<br>SAVE grants authorized federal, state and local benefits-granting agencies and institutions the ability to determine a non-citizen's residency status and thus their G-845 benefits eligibility to receive government provided benefits (e.g., food stamps, unemployment insurance, driver's license, etc.). An individual applying for a benefit provides an agency with their full name, DOB, alien or I-94 number, and identity documents. The agency uses that information, along with the identity document's expiration date, to query SAVE to determine the target's benefit eligibility status. SAVE checks the query information against data already stored in VIS and against various DHS systems. Based on the results of the check, SAVE generates a response code for the agency identifying whether the applicant is eligiblefor benefits, is ineligible for benefits, or has an eligibility status that cannot be determined based on the information provided. Agency use of SAVE is administered by the Verification Division's SAVE Program. Agency registration in the SAVE Program is required to access SAVE. The most recent update to VIS, Release 7.0, added connectivity with the DHS Arrival and Departure Information System (ADIS). Additionally, Release 7.0 introduced the SAVE Case Status Check capability, that allows benefit seeking applicants to view the current status of their case. Release 8.0 introduces benefit eligibility checks based on the grant dates awarded to the Asylums, Lawful Permanent Residents (LPRs), Refugees, and Parolees. |

| | | |
|---|---|---|
| USCIS - Central Index System (CIS) (IRIS) - **The name of the system is CIS2 | USCIS - Central Index System (CIS) (IRIS) - **The name of the system is CIS2 | The CIS serves as a DHS-wide index used to track the location of case files nationally and to maintain alien status and repository information.CIS supports DHS information needs by providing the following four major capabilities: Allows DHS field offices, ports of entry (POE), examination and inspection sites prompt access for accurate biographical and status information on individuals seeking legal entry to or residence in the United States, thus ensuring proper entry and granting of benefits to eligible individuals. CIS also assists the DHS in the identification of individuals who violate the terms of their stay. Identifies the location and timely access to hard copy Alien Files (A-Files) on individuals of interest to the DHS. Serves as a starting point for a system that will move data without the need to move paper A-Files. Provides statistical data and reports to the DHS and other government agencies (OGA). |
| USCIS -Person Centric Query Service (PCQS) | USCIS -Person Centric Query Service (PCQS) | Person Centric Query Service (PCQS) allows users to submit a single query and view all permissible transactions involving an immigrant or nonimmigrant across multiple DHS and external systems. |
| USCIS - Correspondence Handling and Management Planning System (CHAMPS) (Texas Service Center) | USCIS - Correspondence Handling and Management Planning System (CHAMPS) (Texas Service Center) | The Correspondence Handling and Management Planning System (CHAMPS) is used by the Texas Service Center (TSC) to facilitate workflow management, production evaluation, and time and attendance functions. CHAMPS is designed to perform the following case management functions: identify cases that may be delayed because of deficient information or documentation; identify and link multiple petitions and applications to one person and family members of that person; determine the status of those cases; and produce regular and ad hoc reports for management. CHAMPS is used to track USCIS TSC employees' time and attendance information. CHAMPS also serves as an evaluation tool by linking the adjudicator production data. |
| USCIS -Fraud Detection and National Security Data System NexGen (FDNS-DS) | USCIS -Fraud Detection and National Security Data System NexGen (FDNS-DS) | FDNS-DS NEXGEN is a mission critical cCase Management System that maintains the central repository for all data gathered during the processes of administrative investigation, background, identity, and security checks, and analyseis of benefit fraud rates/trends. FDNS-DS NEXGEN allows FDNS Immigration Officers to cross-reference the background, identity, security check, and adjudicative process information for immigration applications, and petitions, or requests with suspected or confirmed immigration fraud, public safety issues, and/or national security concerns. FDNS-DS NEXGEN data is also used to perform statistical analyseis of selected cases for the purpose of identifying benefit fraud rates and trends. (MGT) |

| | | |
|---|---|---|
| USCIS - Computer Linked Application Information Management System (CLAIMS 3) | USCIS - Computer Linked Application Information Management System (CLAIMS 3) | CLAIMS3 is a tracking and processing system used for adjudication of applications/petitions for immigrant benefits and service except asylum and naturalization. USCIS is required to collect fees and adjudicate applications for immigration benefit requests and visas in a timely manner and provide immigration information to various DHS and government entities. To meet these mission requirements, USCIS developed CLAIMS 3 to process immigration benefit requests applications and track information for sharing within DHS and other government agencies. Originally developed to track the receipting of applicant/petitioner payments remittances and to produce notices documenting the payments remittance, C3 functionality now includes adjudication, archive, card production, case history, case transfer, on-demand reports, electronic file tracking, image capture, production statistics, status update and electronic ingest of applicant data captured from the Lockbox and MyUSCIS. CLAIMS 3 receives immigration requests (manually or via electronic ingest), provides ability to adjudicate request, and initiates production of es notices or proof of benefits to customers. |
| USCIS - Alien Change of Address Card (AR-11) | USCIS - Alien Change of Address Card (AR-11) | AR11 / DIS is a web-based solution built on the Coldfusion platform that captures change of address information and then sends it to the AR11 Mainframe. |
| USCIS - Customer Relationship Interface System (CRIS) | USCIS - Customer Relationship Interface System (CRIS) | Customer Relationship Interface System allows customers access to obtain the status of their applications and petitions for immigration benefit requests and processing time information. |
| USCIS - Adoption Case Management System (ACMS) | USCIS - Adoption Case Management System (ACMS) | The Adoption Case Management System (ACMS) module under the National Processing Workflow Repository (NPWR) serves as the case-management system for the domestically-filed intercountry adoption process. ACMS is used by the USCIS National Benefits Center (NBC) to facilitate the effective and efficient processing of domestic intercountry adoption-related applications and petitions. |

| | | |
|---|---|---|
| USCIS - Microfilm Digitization Application System (MiDAS) (IRIS) | USCIS - Microfilm Digitization Application System (MiDAS) (IRIS) | The objective of MiDAS is to enable USCIS personnel to search, retrieve, and deliver information about individuals contained in historical USCIS records to respond to requests received from Federal, state and local Government agencies and the public. Government agencies use information obtained from MiDAS to assist in the determination to grant or deny a Government benefit or to conduct a law enforcement investigation. Members of the public use MiDAS to obtain historical immigration records for genealogical and other historical research. MiDAS is a standalone system which does not share information with other systems. |
| USCIS - Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) | USCIS - Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) | Data & Business Intelligence Services (DBIS) provides two major capabilities to support the USCIS mission. The Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) and the eCISCOR reporting and analytics tool set. eCISCOR is a multi-tier data repository and sources USCIS transactional and derived data from all major USCIS transactional systems. eCISCOR is the official USCIS data warehouse and also serves as a data hub for applications that need data from other systems. The eCISCOR Tool Set includes: Standard Management Analysis & Reporting Tool (SMART) —uses the technology platform Oracle OBIEE and it is a self-service, web based, reporting and analytics tool to develop reports and dashboards derived from source USCIS data sets. SAS Predictive Modeling Environment—SAS PME is suite of SAS™ integrated system of software solutions that enables you to perform the following tasks: data entry, retrieval, and management and statistical and mathematical analysis. eCISCOR BIG Data—uses the Databricks™ platform and big data environment based on Apache Spark technologies to provide a capability to enables teams of Data Scientists to research business questions with eCISCOR data using a variety of tools and languages. eCISCOR BigData Analytics - BigData Analytics (BDA) using Tableau is composed of licensed based creator and user tools and a web server to publish content. BDA excels at visualizing data, unlike some of the other eCISCOR Reporting Tools used throughout USCIS. Additionally, BDA has the capability to merge unrelated datasets together with less effort. BDA uses data from eCISCOR to develop and create analytics and visualizations. Furthermore, BDA can also serve as the means in which eCISCOR BigData data is presented. |
| USCIS - Global | USCIS - Global | Global is a case management system that supports USCIS in the screening of individuals in the credible fear, reasonable fear, affirmative- and defensively-filed asylum applications (I-589), defensive, and NACARA (I-881) processes. It provides the means for tracking of asylum cases as they progress from application filing through final determination/decision or referral to the U.S. Immigration Courts and cases processed for applicants seeking refugee status abroad. (RAIO) |

| | | |
|---|---|---|
| USCIS - Citizenship and Immigration Data Repository (CIDR) | USCIS - Citizenship and Immigration Data Repository (CIDR) | USCIS developed CIDR, hosted on DHS classified networks, in order to make classified and unclassified information from these USCIS systems available to authorized USCIS personnel for the purposes of vetting USCIS application information for indications of possible immigration fraud, public safety, and national security concerns.  CIDR allows authorized users to cross-reference when classified information must be cross-referenced with unclassified data in USCIS data sets to , detecting possible fraud by USCIS employees, including but not limited to potential misuse of immigration information or position by USCIS employees.  CIDR also allows authorized users to and responding to similar tips or referrals received from other federal agencies via classified channels, and responding to requests for information (RFI), based on classified criteria, from the DHS Office of Intelligence and Analysis (I&A) and/or federal intelligence and law enforcement community members. |
| USCIS - Validation Instrument for Business Enterprises (VIBE) | USCIS - Validation Instrument for Business Enterprises (VIBE) | Validation Instrument for Business Enterprises (VIBE) is used to validate the business operations and financial viability of employers seeking to hire foreign workers and identify benefit fraud based on internal and other government agencies’ referrals. USCIS uses VIBE to enhance USCIS adjudications of certain employment-based immigration petitions and applications. VIBE consolidates and displays information from USCIS systems, Dun and Bradstreet, labor certification information from the Department of Labor, and VIBE-generated information based on USCIS developed algorithms through the VIBE Status Report (VSR—a consolidated report generated by a specifically designed algorithm in VIBE). This data helps identify eligible petitioners/employers, as well as ineligible employers and potentially fraudulent filings. VIBE enhances USCIS’s mission by distinguishing eligible petitioners/employers from those that are ineligible. |

| | | |
|---|---|---|
| USCIS - Customer Management Information System (CMIS) (Q-Flow) | USCIS - Customer Management Information System (CMIS) (Q-Flow) | CMIS (Q-Flow) is a computerized queuing system used to facilitate and expedite the processing of the customers in the USCIS waiting areas. Q-Flow CMIS manages customer queuing for service at USCIS district offices. The system can handle appointments, reception and & registration, customer routing and & queuing, service documentation, content management, monitoring, real time alerts, historical analysis and in-depth reporting. Q-Flow is designed to enhance the customer experience and optimize the efficiency of representative agents (ISOs). By incorporating Digital Signage, Q-Flow helps keep customers informed while creating a more relaxed waiting room. Also, real-time alerts and an advanced reporting module allow managers to monitor service conditions without leaving their desks. The system consists of a computer-driven master display, customer ticket printer, and individual counter terminals for each service counter position, including a Reception counter employed in many offices. The effectiveness of USCIS operations depends on the management of the system in every field location as well as Headquarters. Q-Flow doesn't merely sort and manage customers, but it improves the management of customer services by measuring productivity, alerting managers to resource allocation issues, and providing valuable customer service data. As such, leadership within local offices can view real-time status as well as historical data pertinent to operations within the office. This data is shared throughout USCIS – from the 26 Districts, to the 4 Regions and ultimately Headquarters. This allows leadership not only to evaluate operations within Field Offices throughout the United .States., but also the ability to make strategic decisions based on its accurate data captured in the field. The purpose for mission of Q-Flow CMIS is to improve customer experience within USCIS nationwide. |
| USCIS - Case and Activity Management for International Operations (CAMINO) | USCIS - Case and Activity Management for International Operations (CAMINO) | CAMINO is a legacy case management system that supports USCIS in the screening of individuals for protection screenings on the Coast Guard? cutters, and for adjudication of Form I-730 follow-to-join petitions for relatives of Asylees and Refugees, Central American Migrant Parole (CAM) requests, I-590 Requests for Review (RFR), I-602 waivers, I-730 administrative appeals using Form? I-290Bs, and Parole Foreign Government request or referrals for parole referral processes. It provides the means for tracking of work completed in international offices as cases they progress from application filing through final determination. |

| | | |
|---|---|---|
| USCIS - National Customer Service Center (NCSC) | USCIS - National Customer Service Center (NCSC) | The National Customer Service Center (NCSC) to provides nationwide telephonic assistance to customers calling with immigration service and benefit inquiries.  The NCSC uses a wide variety of systems, applications, and tools as part of its call center infrastructure to ensure calls are queued and processed as quickly as possible. Customers includes an applicants, petitioners, employers, attorneys, Community Based Organizations, or any individual calling into NCSC for immigration related information. The NCSC has a multi-tier customer support system that offers recorded and live assistance options. These tiers include the Interactive Voice Response system (IVR), Tier 1 Customer Service Representatives (CSR), and Tier 2 Immigration Service Officers (ISO). USCIS uses a wide variety of systems, applications, and tools to support workflow, data capture, telecommunication functionality, and reporting. |
| USCIS - USCIS Electronic Immigration System (USCIS ELIS) | USCIS - USCIS Electronic Immigration System (USCIS ELIS) | USCIS ELIS is an internal case management system composed of microservices designed to assist with performing complex adjudicative and processing tasks.  These tasks include processing and adjudication actions, such as case receipt and intake, biometric collection appointment generation, case specific processing and management, automated background checks, interview appointment scheduling, final decision rendering, and production of the proof of benefit.  USCIS currently uses ELIS to processing the majority of benefit requests filed with processed by USCIS. |
| USCIS - National Appointment Scheduling System (NASS) | USCIS - National Appointment Scheduling System (NASS) | The goal of National Appointment Scheduling System (NASS) is to provide USCIS with an enterprise-wide appointment scheduling system that will enable USCIS to better address the demands of its existing case load and to better implement new requirements as they emerge. NASS provides a centralized, scalable national appointment scheduling system that will subsume and replace the legacy scheduling mechanisms for fingerprinting, interviews, and oath ceremonies. |

| | | |
|---|---|---|
| USCIS - Customer Profile Management Service (CPMS) | USCIS - Customer Profile Management Service (CPMS) | The Customer Profile Management System (CPMS) is the repository of biometric & background check data for USCIS. CPMS provides the capability to store and reuse biometric images and biographic information about applicants, and initiates background check requests about those applicants. CPMS records biometric and biographic data collected by other USCIS systems, and then uses a combination of biometric and biographic identifiers to determine an applicant's identity in CPMS. CPMS performs biometric vetting to determine which biometrics can be reused based on that identity, and verifies the identity of qualified applicants by sending newly captured fingerprints to DHS-IDENT for verification against previously captured fingerprint images.  Once an identity is verified, CPMS requests background checks from FBI and, depending on the form type, DoD or a foreign partner country. Knowledge of both biometric identification and biographic identifiers at each stage of the process provides a person-centric view of applicants' interactions with USCIS throughout the immigration process. CPMS provides USCIS along with ICE and CBP the capability to search for biometric and biographic information on immigrant applicants. |
| USCIS - Administrative Appeals Office (AAO) Case Management System (CMS) | USCIS - Administrative Appeals Office (AAO) Case Management System (CMS) | The U.S. Department of Homeland (DHS) U.S. Citizenship and Immigration Services (USCIS) Administrative Appeals Office (AAO) uses the AAO Case Management System (CMS) to capture and track information related to appeals, motions, and certifications that AAO adjudicates under its jurisdiction, and to improve its ability to track appeals and case processing.<br>The USCIS AAO developed the AAO Case Management System to track adjudicative work performed by AAO using the Salesforce Government Cloud.1 The Salesforce Government Cloud provides a trusted and secure service to the U.S. Government, and quickly and securely delivers applications to meet customer’s needs. Customers are able to create business applications by tailoring applications built by salesforce.com (Service Cloud, Sales Cloud) or by building their own custom application on the Salesforce platform. The AAO Case Management System is used to track appeals, motions, and certifications filed with or processed by USCIS AAO. |
| USCIS - myUSCIS | USCIS - myUSCIS | An integrated, simplified, transparent digital experience that makes it easy for customers to understand the benefits process, apply for benefits, view information about their case, and contact USCIS for support. |
| USCIS - Enterprise Correspondence Handling Online (ECHO) | USCIS - Enterprise Correspondence Handling Online (ECHO) | Enterprise Correspondence Handling Online (ECHO) is a web-based system that provides employees the ability to generate various types of correspondence, i.e. requests for evidence, denials, etc. ECHO can be used independently or in conjunction with ELIS and other case management systems. ECHO is designed to enhance USCIS customer service, standardize procedures and requirements, and improve information quality and reliability. ECHO's goal is to support the USCIS Mission in the following areas, including but not limited to: Adjudications Analysis and Integrity Enhanced Reporting Capabilities Customer Relations Management Records Management Standardization |

| | | |
|---|---|---|
| USCIS - Global I-590 | USCIS - Global I-590 | USCIS developed Global I-590 to serve as the primary IT case management system to support the International and Refugee Affairs Division (IRAD) within the RAIO Directorate. Global I-590 is a secure, web-based, case management application designed to facilitate the effective and efficient processing of refugee applications referred to and adjudicated by USCIS officers as part of the U.S. Refugee Admissions Program (USRAP). |
| USCIS - IMPACT | USCIS - IMPACT | IMPACT identifies risk factors for an entrepreneur investor case by automating the collection of data from various sources and leveraging that information in a workflow of automated business rules. |
| USCIS - RAILS (IRIS) | USCIS - RAILS (IRIS) | USCIS RAILS allows authorized personnel to track and request internal immigrant files and receipt files.  It supports Records Division Personnel in performing their duties in maintaining and locating Alien Files (A-Files).  Plus, it provides other systems with information about A-File locations and information associated with A-Files.  In addition, USCIS RAILS in combination with other applications provides the Corporate Repository of A-File and Receipt File information. |
| USCIS - Freedom of Information Act (FOIA) Immigration Records System (FIRST) (IRIS) | USCIS - Freedom of Information Act (FOIA) Immigration Records System (FIRST) (IRIS) | FIRST is an electronic case management system with a public facing portal that allow users to submit, manage, and receive FOIA/PA requests entirely Online. The application also allows USCIS personnel and contractors to review and process electronically scanned images of documents responsive to FOIA/PA requests to ascertain and apply apply appropriate FOIA or Privacy Act exemptions. |
| USCIS - Content Management Services (CMS)(IRIS) | USCIS - Content Management Services (CMS)(IRIS) | CMS creates a platform for use across USCIS to manage person-centric, immigration-related electronic content and services.  This platform provides the back-end repository and content services for other USCIS applications to utilize.  It will also be the primary platform for building content-rich applications.CMS delivers enterprise resources, including:  Multiple, related USCIS Content Repositories  Content Service APIs  Content Ingestion Processing  STACKS WebUIAdditionally, CMS provides a cryptographic object storage solution to enable secure deletion of content from AWS and content services specifically focused on the FOIA domain supporting the FIRST system. CMS delivers a modernized content application, including migration of existing A-File content and incorporation of new content repositories, and integrates person-centric concepts as a key component in immigration records management and paperless adjudication. |

| | | |
|---|---|---|
| USCIS - Enterprise Gateway and Integration Services (EGIS) | USCIS - Enterprise Gateway and Integration Services (EGIS) | Enterprise Gateway and Integration Service (EGIS-) is a group of services that offer integration and information sharing capabilities within USCIS, DHS and external partners. EGIS primarily support eProcessing and ESB modernization for USCIS, using up-to date technology to modernize the Enterprise Service Bus (ESB). EGIS provides reference data service, payment service, .PDF (JSON) Form service and encryption service to USCIS in support of the eProcessing services and O&M support using a middle tier for the Enterprise that enables content routing, message orchestration, integration services across the enterprise, build and support event |
| USCIS - Enterprise Collaboration Network (ECN) | USCIS - Enterprise Collaboration Network (ECN) | The U.S. Department of Homeland Security (DHS), U.S. Citizenship and Immigration (USCIS) uses SharePoint-as-a-Service (SharePoint), commonly referred to throughout the agency as the Enterprise Collaboration Network (ECN), a web browser-based collaboration and document management platform from Microsoft. The USCIS ECN is a secure space for USCIS employees to create, manage, and share documents using customizable tools and services to eliminate additional investments in duplicative collaborative technologies. The USCIS ECN supports secure agency-wide collaboration and communication by connecting separate USCIS Program Offices and Directorates located in various geographic areas through the use of a common platform |
| USCIS - ATLAS | USCIS - ATLAS | USCIS developed ATLAS to automate, streamline, and support accurate exchange of data among USCIS, DHS, and non-DHS systems used to support biometric-and biographic-based screening of immigration requests. ATLAS supports the vetting of immigration requests, which may include information related to the applicant, beneficiary, petitioner, sponsor, or other individuals associated with an immigration request. ATLAS is not used as a case or content management system and therefore does not have “users” in a traditional sense. ATLAS serves two primary purposes: background check services and rule-based screening. |
| USCIS - Pangaea | USCIS - Pangaea | This tool provides RAIO adjudicators with quick access to country of origin iInformation (COI) and suggested lines of questioning for applicants. |
| USCIS - Person Centric Identity Services (PCIS) | USCIS - Person Centric Identity Services (PCIS) | PCIS is a single, trusted, authoritative source of biographical and biometric information used to holistically link and maintain all elements of applicants, petitioners, beneficiaries as well as representatives, interpreters, preparers, sponsors, civil surgeons and others. To create this comprehensive, person-centric view of individuals, PCIS includes data, system architecture, and user functionality from the Central Index System (CIS2) and Person Centric Query Service (PCQS), person data from USCIS systems (e.g., case management systems) as well as integration with the Customer Profile Management System (CPMS). The comprehensive person data is stored in an identity index, which contains an individual's immigration history, status, and biographic and biometric identity information. |