

Component	System Name	System Description
ICE	P25 Land Mobile Radio Network	Project 25 (P25) Land Mobile Radios and related Infrastructure will provide mission-critical tactical communications capabilities. The communication technologies will support ICE LEOs in routine operations, continuity of communications, special operations, and emergency response and recovery. TACCOM will provide P25 interoperable communications with all ICE, and all federal, state, local and tribal law enforcement agencies across wide geographic areas. The systems will be scalable and expandable to support tactical communications in emergency situations.
ICE	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. 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.
CBP	CBP Enterprise Monitoring Tools	CBP Enterprise Monitoring Tools (CEMT) is a Major Application that provides monitoring and alerting for situational awareness of CBP's enterprise and system configuration environment. CEMT is a complex system that consists of a combination of Commercial off the Shelf (COTS) applications/software, custom code, and database servers that form various functional areas. Each functional area has its own unique function which shares data throughout CBP with Office of Information and Technology (OIT) managers, CBP Situation Room Personnel, Technical Operations Center (TOC), and the Enterprise Management and Monitoring (EMM) Section.

CBP	CBP Network Operations Center	<p>The CBP Network Operations Center (NOC) is tasked with providing and maintaining technical support on a 24X7 basis for CBP Network. The CBP NOC environment includes CBP field site LAN Switches, WAN optimization appliances, firewalls, DNS DHCP services, engineering services to perform network support, monitoring, and maintenance on NDC-1 Data Center and all CBP field site environments. The CBP LAN switch environment encompasses all manageable switches within NDC NOC enclave and CBP field sites. The purpose of the CBP NOC is to maintain the performance, management and administration capabilities of CBP network, all CBP field site locations to include the underlying switched layer 2 and layer 3 supporting environment. To support this effort of network management, the CBP NOC deploys and maintains all network devices, and collects and report information related to the overall health of the network. Other functions of the NOC include collecting system logs, monitoring network status via polling, archiving historical network, providing Domain Name Service (DNS) resolution for CBP and CBP field sites. To ensure the viability of the NOC, prevention controls have been implemented. Prevention controls include preventing attacks through the use of deploying firewall rules and Switch/Router Access Control Lists (ACLs). Additionally, back-up and recovery procedures help ensure any potential intrusions have minimal impact on these systems.</p>
TSA	Computer Network Defense System	<p>The Computer Network Defense System (CNDS) provides real-time monitoring of system, network, and cyber security events in the TSA Security Operations Center (SOC). Security events are collected via Splunk, a security information and event management system that captures and correlates real-time data in searchable repositories from which it can generate reports and alerts. CNDS primarily stores machine generated security events coming from the IT enterprise network technology stack. This usually consists of Intrusion Detection Systems (IDS), web proxies, firewalls, simple mail transport protocol (SMTP), Anti-Virus (AV) and operating system security and audit event logs. All of this log information is ingested by the CNDS Security Information and Event Management (SIEM) system where it is subjected through a series of detection and correlation rules in order to find the potential threats, suspicious behavior and malicious code that requires further investigation by a TSA SOC analyst.</p>