# Customs and Border Protection (CBP)

U.S. Customs and Border Protection

**Mission:** CBP is one of the world's largest law enforcement organizations and is charged with safeguarding America's borders, thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel.

**Cyber Snapshot:** CBP cybersecurity experts provide operational day-to-day technology support and security to all CBP field locations, technology training, enterprise wide area network, security operations and helpdesk services. CBP digital forensic examiners conduct complex analyses of electronic media, develop innovative tools and methodologies for data extraction, detection of unlawful activity, and provide onsite field support and training to law enforcement officers. CBP also conducts analyses into suspected computer hardware and software/code for patent and trademark infringements.

## Customs and Border Protection (CBP) – Office of Information and Technology (OIT)

**CBP- OIT** is especially interested in applicants that have completed coursework or previous work assignments related to: malware analysis; forensic analysis; threat analysis; risk assessment; intelligence analysis; incident response; hardware; network monitoring/network defense; virtual environments; security assessments; basic knowledge and understanding of cybersecurity policies, plans, and standards, mobile applications, and basic curiosity about how things work, open source LINUX tools like KALI, assistance with IT systems accreditation, security test and evaluation, policy and training; to gain experience with several projects/tasks to improve security operations, monitoring, automated workflows, and incident response/forensics. Interested students should have relevant coursework, Microsoft Office, computer engineering and information technology (IT) basics.

**CBP OIT Offices:**

- **Cyber Security Directorate (CSD)**
  - Security Operations Division (SOD) -Alexandria, VA
  - Security and Policy Division (STP) - Falls Church, VA
- **Enterprise Data Management and Engineering Directorate (EDMED)**
  - Springfield, VA
- **Border Enforcement Management Systems Division (BEMSD)**
  - Candidates will participate at the Alexandria, VA (Walker Ln) office

**CBP OIT - Cyber Security Directorate (CSD):** The Cyber Security Operations Center (CSOC) requests research participants to learn and gain experience in critical efforts in security operations and security sustainment with DHS. Participants within the CSOC will bring new perspective on organizational issues and fresh, new ideas with their understanding of emerging technology and security issues. Participating in the DHS CSVI

program exposes students to real world issues and is a great way to help them determine how much potential they have in the IT security field. CSOC is currently seeking research assistance with several projects/tasks related to improving security operations, monitoring, automated workflows, and incident response/forensics. We welcome students with experience with new technologies, especially mobility technology and its challenges.

**CBP OIT Security and Technology Policy (STP):** The Security and Technology Policy (STP) branch secures the CBP IT environment by assessing security risks and vulnerabilities, implementing DHS and CBP information system (IS) security policy, and overseeing the CBP Security Program. Coordinating OIT Audit activities and overseeing IT Security Policy, STP is composed of project teams involved in all aspects of Automated Information System security administration to support the CBP mission and management priorities.

**Security and Technology Policy Areas of focus:**

IT Systems Certification and Accreditation (C&A)

- C&A status reporting
- Review Mission Interconnection Security Agreements
- Process DHS and CBP security policy Waivers and Exceptions

Risk Assessment

- Risk Assessments Tracking
- Security Compliance Inspections and Security Audits Support
- Security Audit Corrective Action Plans Monitoring and Reviews

Security Test and Evaluation

- Draft Security Assessment Plan
- Perform vulnerability scans
- Analyze results of testing actions

Policy and Training

- Tracking Training Compliance
- Development and updates of CBP Security Policies

## CBP OIT- Enterprise Data Management and Engineering Directorate (EDMED)

*Enterprise Data Center Operations Branch (EDCOB):* The EDCOB manages and oversees data center facilities and IT operations activities that support the DHS and CBP missions. The services provided by EDCOB include supporting the CBP Cloud Computing Environment, mobility operations, identity and credential management platforms, UNIX and Windows servers and the Mainframe, managing enterprise storage operations, managing the data center local area network and its operations, engineering and operations of database and information management, Situation Room operations and reporting, 24/7/365 enterprise operations center operations, and enterprise monitoring and change control board. EDCOB also has responsibility for working with the Enterprise Systems Engineering Branch to consolidate servers, modernize operations, and be a full service provider to OIT, CBP, and its customers.

Participants will learn to perform tasks such as: documenting action items, processes and procedures; incident management, documenting actions taken as well as identifying POCs during incident resolutions; and, content management in SharePoint. Relevant coursework: Microsoft Office, computer engineering/IT basics preferred.

### CBP OIT- Border Enforcement Management Systems Directorate (BEMSD):

The mission and goals of the BEMSD program office is to provide concentrated support for Border Enforcement Systems, for the U.S. Border Patrol, Field Operations, Air and Marine Operations, while also supporting Management Systems solutions for the Office of Administration, the Office of Professional Responsibility, the Office of Human Resource Management and the Office of Training and Development. Responsibilities include system development (for the full life cycle from planning through deployment), of all Border Enforcement and Mission Support systems.
Participants would gain experience with tasks such as: Audit log monitoring being set up to capture event types required by DHS security policy, with the threshold levels for anomalous behavior. Our participant would participate alongside the program Information System Security Officers and development teams who review audit log data, verify that the collected data conforms to DHS security policy requirements, analyze the data to adjust the threshold levels for anomalous behavior, as required, and then look for any associated events that correlate to the captured audit event types.

## Customs and Border Protection (CBP) – Office of Professional Responsibility (OPR) Investigate Operations Division, Cyber Investigations

The mission of U.S. Customs and Border Protection (CBP), Office of Professional Responsibility (OPR) is to "To safeguard and promote the integrity and security of the CBP workforce." Cyber Investigations is a growing component within OPR. The student participant will gain experience in areas related to the investigation of administrative or criminal allegations involving CBP personnel, which consists of approximately 60,000+ employees and contractors, all of which have access CBPs computer network.

Cyber Investigations supports twenty-two OPR field offices, as well as other divisions within CBP assisting with investigations based on allegations of criminal and administrative IT misconduct. Participants may gain experience learning: Cyber case management, IT purchasing, IT Inventory, analysis of program metrics, budget planning, computer hardware/software maintenance relating to computer forensic tools, and the development of policy. In addition, students will have the opportunity to experience computer forensics analysis, as well as performance of evidence intake, processing and analysis with a mentor.

CBP OPR is especially interested in students that have completed coursework or previous work assignments related to: Digital Forensics, IT statistical analysis, program management, project management, and inventory.