Transportation
Security
Administration

Transportation Security Administration (TSA)

Mission: TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. Being a high performing counterterrorism organization, TSA also provides the most effective transportation security in the most efficient way.

Cyber Snapshot: TSA cyber professionals focus on protecting TSA information, data source codes, and information systems against unauthorized access, unauthorized use, unauthorized modification, disclosure, disruption, and destruction. TSA also leads transportation cybersecurity threat analysis for six transportation modes: aviation, freight rail, highway and motor carrier, mass transit, pipeline, and maritime.

TSA is especially interested in students that have completed coursework or previous work assignments related to: malware analysis; incident response; network monitoring/network defense; hardware; network security testing; application security testing; new technology security evaluations; cybersecurity research and technical writing; training and outreach; analysis of raw vulnerability results; project management skills; and those enrolled in a degree program in IT; or those pursuing CompTIA A+ certification.

Computer Network Defense

CND performs real-time analysis of security event logs, the coordination of response to computer security incidents, the independent verification and validation of the security devices protecting the TSA networks, the aggregation and analysis of computer security intelligence (open source and classified), and the evaluation of emerging information technology products and services**.**

Cyber security Awareness and Outreach

Gain an understanding of TSA's mission as the Sector Specific Agency. Students will expand their knowledge of cyber related policies based on Presidential Executive Orders effecting the agencies position as the Sector Specific Agency.

Gain hands on experience related to social engineering of the agency utilizing the tools available within the branch. Contribute to the development of concepts and ideas for TSA's monthly awareness campaign which communicates a specific aspect of cyber security via educational flyers that are posted monthly throughout the elevators and via digital signage at HQ, in addition to posters and other educational messaging to be used across HQ and the field.

Focused Operations

Focused Operations has the vital knowledge of proper evidence handling procedures to include Chain of Custody in the event of an incident within TSA. They understand write blocking technologies and perform hard drive duplications as well as perform data recovery operations to retrieve lost data from the network drive and local hard disks. Focused Ops has the abilities in the area of insider threat, eDiscovery, and digital media analysis.

Operations and Engineering

Cyber Security Projects for the Operations and Engineering Team vary but may include placements with mentors where you will learn and gain experience: updating security devices/software, current end point protection software, updates or replacement to current firewall; testing to ensure systems are designed and implemented in accordance to requirements; conducting User Acceptance Testing (UAT) and defect tracking; collaborating with end-users and other TSA stakeholders to develop approach, status, results and potential impact of testing and quality assurance reviews.

TSA HQ/Secure Infrastructure and Vulnerability Management

The Secure Infrastructure and Vulnerability Assessment Management team is tasked with performing the technical piece of the Security Testing & Evaluation (ST&E) for TSA and non-TSA (contractor managed) systems as well as providing enterprise-wide security oversight, infrastructure support, guidance, and reviews for the TSA IT environment.

TSA Compliance

The Assessor Services Team focuses on “green” compliance with the Security Authorization metric of the DHS FISMA Scorecard. This team supports the transition to Ongoing Authorization and support for the DHS Continuous Diagnostics and Mitigation (CDM) program and associated tools forthcoming to all Components. The team also supports monthly analysis associated with other scorecard metrics as outlined in the DHS Performance Plan.

The Audit Team under Information Assurance and Cyber Security Division is tasked with conducting technical audits to ensure the integrity of the TSA Network and related systems. We monitor Privileged Users Accounts and help ensure only those with the requisite responsibilities are provided access. The student participant with this component would be located at the Walker Lane facility.