Cybersecurity

Science and Technology

THE CHALLENGE: SAFEGUARDING THE NATION'S CRITICAL ASSETS

The increasing use of communication technologies relying on complex data, technology, communication, and interconnectivity has expanded attack surfaces and increased the potential risk of malicious exploitation of government, citizen services, and critical infrastructure. The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cybersecurity Program within the Office of Mission and Capability Support leverages multidisciplinary expertise to research, analyze, and develop cutting-edge cybersecurity technologies and capabilities to improve the protection and resilience of our national critical infrastructure (CI) and federal and state departments and agencies. This program conducts research and development (R&D) in coordination with the DHS Cybersecurity and Infrastructure Security Agency (CISA) in two areas: Cyber Data Analytics and Cybersecurity for Law Enforcement.

Cyber Data Analytics: CISA operational units are challenged to query real-time operational threats. Cyber Data Analytics R&D combines cyber risk analysis with assessments of physical and infrastructure risks, and blended cyber-physical risks and threats. Cyber Data Analytics R&D enhances the ability of operational units to correlate threat intelligence and risk data. This includes performing data analytics, leveraging artificial intelligence (AI) and machine learning (ML) to automate tools and capabilities, and augmenting risk-informed decision making.

Cybersecurity for Law Enforcement: A significant barrier for DHS components with a law enforcement mission is adapting to constantly evolving technologies used in criminal enterprise tactics, as well as technologies and tools used to counter or investigate those activities. New technologies, modalities, and training are required to equip and enable law enforcement to counter these evolving threats.

SOLUTION: CYBER DATA ANALYTICS AND CYBERSECURITY FOR LAW ENFORCEMENT

The S&T Cybersecurity Program addresses these needs through its Cyber Data Analytics and Cybersecurity for Law Enforcement projects.

The Cyber Data Analytics area applies computational analytics and information sharing to improve homeland security cybersecurity risk analysis across government, the 16 Critical Infrastructure Sectors, and the 55 National Critical Functions. The work supports next-generation CISA architectures, computation, and decision-making capabilities, and establishes the foundation for future AI-based cybersecurity solutions. Project activities include: developing representative data sets and joint computational sandbox testing capabilities, assessing analytics tools, experimenting with a variety of use cases, and establishing secure multi-party computational capabilities. Priority focus areas include cyber data analytics tools, software assurance supply chain, and cyber ML.

The Cybersecurity for Law Enforcement project supports the research, analysis and development of new technologies, capabilities, and standards to assist law enforcement in training, prevention against cyber-attacks, cyber-crime investigations, and the forensic analysis of technologies used in criminal activity.

PROGRAM IMPACTS

The Cybersecurity Program "Science for Mission" approach promotes a collaborative relationship between S&T and its operational partners to systematically evaluate and address capability demands in cybersecurity, artificial intelligence and machine learning, and law enforcement. Through this relationship, the Cybersecurity Program's work in these areas enables CISA to meet the objectives outlined in the CISA Strategic Technology Roadmap 2023-2027.

UPCOMING MILESTONES

- Deliver the capability to create and use high-fidelity deception environments to identify adversarial tools, techniques, and practices, which can be provided as threat intelligence to network defenders. (FY23 4th quarter).
- Deliver a study with recommendations for high-performance, distributed, large-scale analytics for application to CISA use cases. (FY23 4th quarter)
- Provide a demonstration of a seamless, multi-cloud sandbox environment for developing rapid analytics for CISA missions. (FY23 4th quarter).