Cybersecurity

Science and Technology

THE CHALLENGE: SAFEGUARDING THE NATION'S CRITICAL ASSETS

The increasing use of communication technologies that rely 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 (MCS), 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 Needs: CISA operational units are challenged to query real-time operational threats. Cyber Data Analytics R&D will combine cyber risk analysis, physical and infrastructure risk, and blended cyber-physical risk/threat. Cyber Data Analytics R&D will enhance the ability of operational units to correlate this 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 situational awareness of risks.

Cybersecurity for Law Enforcement Needs: New communications technology, both hardware and software, is released into the market rapidly, where it is used in criminal and terrorist activity almost immediately. Some of the threats being encountered include anonymous networks and currencies, cyber security forensics tools, Internet of Things, and cyber-attacks against critical infrastructure.

SOLUTION: CYBER DATA ANALYTICS AND CYBERSECURITY FOR LAW ENFORCEMENT

The Cybersecurity Program aims to meet 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. Some 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 will improve our partners' ability to achieve mission success by:

- Improving operational utilization of large and complex data with data analytics techniques and tools
- Enhancing risk analysis, consequence analysis, and threat intelligence data capabilities that will improve cybersecurity incident response times

UPCOMING MILESTONES

- Complete initial build for multi-cloud environment for next generation CISA architecture (Fiscal Year 2022)
- Expand the advanced ML CISA environment to support additional infrastructure security use cases (FY22)
- Deliver capability advances to CISA that combat sophisticated, covert, and targeted malware developed by advanced threat adversaries (FY22 4th quarter)