Homeland Security
Science and Technology

S&T IMPACT: CYBERSECURITY

The **Department of Homeland Security (DHS) Science and Technology Directorate (S&T)** is the primary research and development arm for DHS's operational components and the nation's first responders. S&T helps improve the safety and effectiveness of homeland security professionals by developing innovative solutions with public and private sector partners. **Our approach involves:**

1. IDENTIFYING NEEDS
by discussing operational challenges with DHS components and first responders

2. DEVELOPING PROTOTYPES
or leveraging existing technologies to quickly find solutions

3. TESTING AND EVALUATING
potential solutions to ensure they meet end-user needs

4. DEPLOYING SOLUTIONS
to the field within a short timeframe

S&T helps improve cybersecurity capabilities through strategic research and development (R&D) in the areas of mitigation, solution development and resilience. In line with the **DHS Cybersecurity Strategy**, S&T brings together leading innovators in academia, industry and government to identify new tools and tactics that can help network owners and operators overcome emerging cyber-threats.

RESILIENCE

S&T strengthens security on the Internet of Things (IoT)

- The **Cyber Physical Systems Security (CPSSEC)** project addresses security concerns to protect IoT-connected systems in automobiles, medical devices and building controls.
- The **Smart Cities** project oversees the Global City Teams Challenge with the National Institute of Standards and Technology to improve cybersecurity for smart city systems.

S&T protects mobile devices from evolving cyber threats

- The **Mobile Application Security** project helps incorporate security-by-design into mobile app security tools that assist developers, analysts and security and network operators.
- The **Mobile Device Security** project promotes safe and secure adoption of mobile technology within DHS and across the federal government.

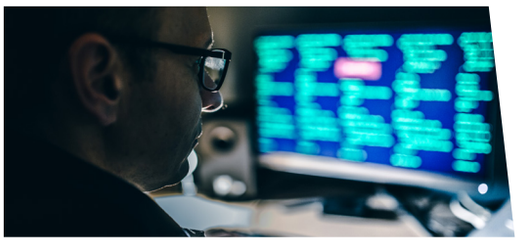
S&T helps secure networks from cyber attacks

- The **Distributed Denial of Service Defense** project deploys best practices that can help slow attack scale growth and defend emergency management telephony systems.
- The **Federated Security** project brings together voluntary teams of organizations to share information and resources that can strengthen their cybersecurity capabilities.

SOLUTION DEVELOPMENT

S&T makes it easier for law enforcement to investigate cyber crimes

- The **Anonymous Networks and Currencies** project develops new cost-effective solutions to help law enforcement agencies investigate criminal activity taking place on anonymous networks and with cryptocurrencies.
- The **Cybersecurity Forensics** project develops tools and techniques law enforcement can use to investigate criminal and terrorist activity on mobile devices, GPS units and more.



S&T promotes cutting-edge cyber research

- The **Cyber Risk Economics (CYRIE)** project supports research into the business, legal, technical and behavioral aspects of cyber threats to improve decision-making for critical infrastructure owners and operators.
- The **Information Marketplace for Policy and Analysis of Cyber risk and Trust (IMPACT)** facilitates information-sharing among the global cybersecurity R&D community.

MITIGATION

S&T keeps critical infrastructure up and running

- The **Next Generation Cyber Infrastructure (NGCI) Apex program** is addressing the cyber challenges facing our nation's critical infrastructure sectors to prevent adversaries from infiltrating our systems through the development of tools and technologies.
- The **Distributed Environment for Critical Infrastructure Decision-making Exercises (DECIDE)** project is advancing state-of-the-art critical infrastructure protection exercises to prepare an effective response to a high-consequence financial sector event.

S&T strengthens software starting in the development phase

- The **Application Security Threat and Attack Modeling (ASTAM)** project makes it easier to identify potential cybersecurity risks through automated software analysis.
- The **Software Assurance Marketplace (SWAMP)** provides secure, dependable analysis to help reduce the number of vulnerabilities deployed in new software systems.
- The **Software Quality Assurance** project addresses challenges with software security analysis and coding to help eliminate weaknesses early in the development process.

S&T relies on partnerships with industry, academia and technology developers to continue providing **next-generation solutions** that improve responder safety and effectiveness. If you're interested in helping strengthen the nation's homeland security, visit our **Business Opportunities** page to discover the many ways to work with S&T. Then, check out the rest of our website and follow S&T on **Facebook**, **Twitter**, **YouTube**, and **LinkedIn** for the latest updates on our work.

scitech.dhs.gov

dhsscitech