Cyber Security Division

Securing Your Cyber Future

2017 Portfolio Guide

Homeland Security

Science and Technology

Table of Contents

Cyber Security Division Overview

The nation's economic strength and security rely heavily on a vast array of interdependent and critical networks, systems, services and resources to conduct daily business and transactions. These most important assets face continuous threats from cyberattacks.

At the Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Homeland Security Advanced Research Projects Agency, the Cyber Security Division (CSD) enables and supports research, development, testing, evaluation and transition of advanced cybersecurity and information assurance technologies. CSD's portfolio aligns with the federal government's Federal Cybersecurity Research and Development Strategic Plan announced in February 2016.

2014 Quadrennial Homeland Security Review

DHS has identified strengthening the security and resilience of cyberspace as a priority in the 2014 Quadrennial Homeland Security Review. The four priority areas for safeguarding and securing cyberspace are the following:

- Strengthen the security and resilience of critical infrastructure
- Secure the federal civilian government information technology enterprise
- Advance law enforcement, incident response and reporting capabilities

Mission

CSD develops and delivers new cybersecurity research and development (R&D) technologies, tools, techniques, and next-generation cybersecurity capabilities that enable DHS and the nation to defend and secure current and future critical systems and networks against cyberattacks.

Cybersecurity and resiliency are global concerns. CSD leverages public-private partnerships to identify real-world requirements for innovative technology solutions, which are developed with the partners and transitioned into the marketplace.

Website: U.S. Department of Homeland Security Cyber Security Division

- Strengthen the ecosystem:
  - Drive innovative and cost effective security products, services and solutions throughout the cyber ecosystem
  - Conduct and transition research and development, enabling trustworthy cyber infrastructure
  - Develop skilled cybersecurity professionals
  - Enhance public awareness and promote cybersecurity best practices
  - Advance international engagement to promote capacity building, international standards and cooperation

Cyber for Critical Infrastructure

Critical Infrastructure Design and Adaptive Resilient Systems (CIDARS)

The Critical Infrastructure Design and Adaptive Resilient Systems project is a new initiative focused on enhancing the security and resilience of critical infrastructure systems consistent with Presidential Policy Directive 21 and the National Critical Infrastructure Security and Resilience Research and Development Plan. This project is examining innovative approaches to plan and design adaptive performance into critical infrastructure systems. The goal is to create common capabilities and quantitative approaches that facilitate the development and implementation of integrated solutions that will enable secure and resilient service provisioning.

The Critical Infrastructure Resilience Institute

A DHS Center of Excellence – The DHS Science and Technology Office of University Programs manages a network of Centers of Excellence, which conduct research to address homeland security challenges. Infrastructures increasingly are linked through new business models and technologies in an ever-changing threat environment. The University Program's Critical Infrastructure Resilience Institute (CIRI) Center of Excellence was established to explore cyber asset dependencies within the critical infrastructure's organization, policy, business and technical models and conduct research and education to enhance the resilience of the nation's critical infrastructure and its owners and operators. The CIRI is collaborating with industry, DHS and other federal and state agencies in four cyber research themes: understanding resilient infrastructure systems, application of critical infrastructure in the real world, building the business case for resilience, and the future of resilience.

Websites: **Critical Infrastructure Resilience | Homeland Security University Programs**

Cyber Resilient Energy Delivery Consortium

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure. The electric grid faces challenges from cyberattacks, natural disasters and accidental failures. To address these challenges, CSD and the Department of Energy (DOE) jointly fund the Cyber Resilient Energy Delivery Consortium (CREDC). The consortium is developing solutions through R&D, education and industry engagement. CREDC will generate research, evaluate the results and deploy solutions in the marketplace. The project's foci include cyber protection technologies; cyber monitoring, metrics, and event detection; risk assessment of Energy Delivery Systems (EDS) technology; data analytics for cyber event detection; resilient EDS architectures and networks; and identifying the impact of disruptive technologies such as the Internet of Things and cloud computing on EDS resiliency.

Website: **CREDC: Cyber Resilient Energy Delivery Consortium**

Distributed Environment for Critical Infrastructure Decision Making Exercises

The nation's financial infrastructure is one of the most lucrative targets for cyber criminals. Successful attacks could be disruptive to the nation's daily economic activities. To help secure this sector from cyberattacks, CSD developed the Distributed Environment for Critical Infrastructure Decision Making Exercises (DECIDE) project—a national cyber war-gaming capability. This project has delivered simulation-supported cyber exercises to critical infrastructure owners and operators, enabling them to create and run exercises that are relevant to their business interests.

Website: **U.S. Department of Homeland Security Distributed Environment for Critical Infrastructure Decision-making Exercises**

Cyber Physical Systems

Cyber Physical Systems Security

Cyber physical systems are smart networked systems with embedded sensors, processors and actuators that sense and interact with the physical world, including humans. Device manufacturers and operators are increasingly seeing the potential of adding computational power and network connectivity to a wide range of devices including vehicles, power grids, medical devices, building controls and many more systems, however, often security is overlooked. The Cyber Physical Systems Security project's goal aims to help ensure security considerations are built into the design while cyber physical systems are still emerging.

Website: U.S. Department of Homeland Security Cyber Physical Systems Security

Cybersecurity Outreach

Cybersecurity Competitions

Ensuring that the nation has a highly skilled cybersecurity workforce is important to maintaining its systems and networks and combating future cyberattacks. The Cybersecurity Competitions project's objective is to lay the groundwork for a thriving future cybersecurity professional community by exposing high school and college students to robust and engaging cyber competition challenges. These competition environments also expose the students to cutting-edge cyber defense tools and technologies developed within CSD.

Websites: U.S. Department of Homeland Security Science and Technology Cybersecurity Competitions

National Collegiate Cyber Defense Competition

U.S. Cyber Challenge

Cybersecurity Research Infrastructure

Experimental Research Testbed (DETER)

It is important that new cybersecurity approaches are evaluated in a realistic environment. The Experimental Research Testbed, also known as the DETER testbed, enables cybersecurity researchers to run their experiments on a "virtual Internet." This self-contained environment allows researchers to test advanced defense solutions safely against "live" threats without endangering other research or the larger Internet.

Websites: U.S. Department of Homeland Security Experimental Research Testbed
The DETER Project

Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT)

The IMPACT project supports the global cyber-risk research community by coordinating and developing real-world data and information-sharing capabilities including tools, models and methodologies. To accelerate solutions around cyber-risk issues and infrastructure support, the IMPACT project coordinates data and information sharing between the government, critical infrastructure providers and the cybersecurity research and development community.

Website: Impact Cyber Trust

Human Aspects of Cybersecurity

Cyber Economic Incentives

Despite the growing national focus on cybersecurity, there has been little attention from the research community on economic, behavioral and business factors that persuade a private organization to select and implement cybersecurity measures. The Cyber Economic Incentives project examines where, why and how much cyber-infrastructure owners and operators should invest in cybersecurity. This project is researching adoption incentives, the reputations of commercial network operators for preventing attacks and understanding criminal behaviors to mitigate risks.

Website: U.S. Department of Homeland Security Cyber Risk Economics (CyRiE)

Incident Response Communities

Cybersecurity Incident Response Teams (CSIRTs) are vital to responding to network events and mitigating damage and consequences. The Incident Response Communities project has created an interdisciplinary team of cybersecurity and software researchers, organization psychologists, economists and practitioners to determine and validate the principals of creating, running and sustaining an effective CSIRT team.

Website: U.S. Department of Homeland Security Cyber Security Incident Response Teams

Insider Threat

Cybersecurity defenses most often focus on threats from outside an organization, rather than threats posed by untrustworthy insiders even though insider threats frequently are the source of loss of financial or sensitive information and harm to critical infrastructure industries and national security. The Insider Threat project is developing approaches to detect and mitigate insider threats that will benefit a wide range of government and private-sector customers.

Website: **U.S. Department of Homeland Security Science and Technology Insider Threat**

Usable Cybersecurity

Implementing and operating secure systems can be difficult for the common user and the trained professional, particularly when balancing tradeoffs between security and functionality. The Usable Cybersecurity project's goal is to develop intuitive security solutions that can be implemented easily by IT owners and operators with limited or no training required.

Website: **U.S. Department of Homeland Security Science and Technology Enterprise Level Security Metrics and Usability**

Identity Management and Data Privacy

Identity Management

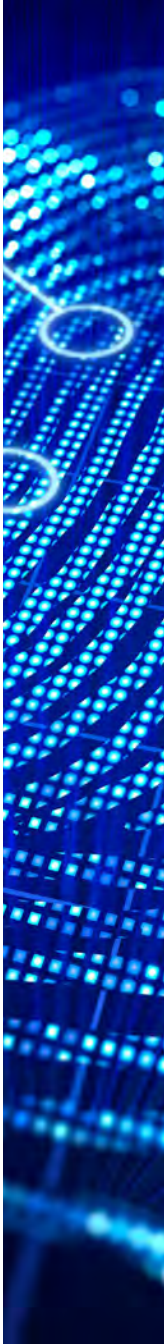
The Identity Management project develops, tests and evaluates interoperable tools, technologies and standards to help manage authentication, identification, access control, fraud analytics and compensating controls. This project seeks to identify solutions to increase security and productivity, while reducing costs and security risks.

Website: U.S. Department of Homeland Security Science and Technology Identity Management

Data Privacy

The Data Privacy project develops, tests and evaluates tools and standards for the management of personally identifiable information (PII), automation of privacy controls, privacy implications of connected devices, big data and anomaly detection. It is working to ensure the protection of personal information consistent with public policy.

Website: U.S. Department of Homeland Security Science and Technology Data Privacy



Law Enforcement Support

Anonymous Networks & Currencies

Criminals are increasingly exploiting the privacy-enhancing protections built in for the legitimate use of anonymous networks and cryptocurrencies. Criminal investigations of anonymous networks and cryptocurrencies are resource intensive and challenging, requiring the investment of significant person-hours to investigate and prosecute. The Anonymous Networks & Currencies project works with the law enforcement community to develop cost-effective solutions to complement and expand their abilities to investigate online criminal activity.

Website: **U.S. Department of Homeland Security Science and Technology Anonymous Networks Currencies**

Cybersecurity Forensics

Almost all criminal investigations today include digital evidence. As a result, law enforcement officers and forensic analysts face a constant need to keep pace with technology advancements. The Cybersecurity Forensics project works with the law enforcement community to gather requirements and develop cost-effective solutions and capabilities to facilitate the quick acquisition and analysis of information from a wide variety of electronic devices, including cell phones, GPS devices, tablets and vehicle infotainment systems.

Website: **U.S. Department of Homeland Security Science and Technology Cyber Forensics**

Mobile Security

Mobile Application Security

Mobile applications offer government and business opportunities to improve mission effectiveness and productivity by providing always-on connectivity, real-time information sharing and unrestricted mobility. However, because of the increasing use of mobile apps to access information and services, apps are replacing operating systems as the most prominent avenue of cyberattack, misuse and unauthorized exfiltration of data (e.g., PII). The Mobile Application Security project will identify innovative approaches that extend beyond app deployment to provide continuous validation and threat protection as well as enable security throughout the mobile app lifecycle.

Website: U.S. Department of Homeland Security Science and Technology Mobile Device Security

Mobile Device Security

Mobile technology has changed how people communicate, make daily decisions and execute business transactions. However, the lack of security has prevented enterprise organizations from fully embracing mobile technology. The Mobile Device Security project is developing innovative security technologies to accelerate the secure adoption of mobility for mission use. The project is comprised of three R&D areas—software-based mobile roots of trust, mobile malware analysis and application archiving, and mobile technology security such as device instrumentation, secure transactional methods, management tools and device layer protection.

Website: U.S. Department of Homeland Security Science and Technology Mobile Device Security

Next Generation Cyber Infrastructure Apex Program

NGCI Apex

Cyberattacks threaten national security by undermining information-dependent critical infrastructure. The Next Generation Cyber Infrastructure (NGCI) Apex program addresses financial services sector challenges by providing the technology and tools to counter advanced adversaries when they attack U.S. cyber systems and financial networks. The NGCI Apex program concentrates on delivering capabilities in five primary functional gap areas: Dynamic Defense, Network Characterization, Malware Detection, Software Assurance and Insider Threat. To accomplish its mission, NGCI Apex identifies tests, evaluates and deploys new technologies that deter cyber intrusions across financial sector networks.

NGCI Apex leverages existing federally funded and private-sector research efforts that meet the capabilities to defend against sophisticated, targeted cyberattacks. The program uses a flexible and repeatable development approach to forage for candidate technologies. Once technologies are identified, the NGCI program launches testing and evaluation before developing a transition path into the marketplace. Financial institutions can adopt any transition-ready technologies that are best suited to their enterprise operations.

Website: U.S. Department of Homeland Security Science and Technology Protecting the Nation's Cyber Infrastructure

Network and System Security

Distributed Denial of Service Defense

Distributed denial of service attacks are growing and frequently target critical infrastructure sectors and government agencies. The goal of the Distributed Denial of Service Defense project is to slow attack growth by promoting best practices and building technologies to mitigate new and current attack types. Through these strategies, critical infrastructure sectors and government agencies will have the ability to withstand one terabit per second attacks. This new level of defense will push the defender into the lead.

Website: U.S. Department of Homeland Security Science and Technology Distributed Denial of Service Defense (DDoSD)

Enterprise Level Security Metrics

Developing meaningful cybersecurity metrics has been challenging, particularly as information technology and cyberattack methods change and evolve. This constantly changing environment makes it difficult for organizations to evaluate effectively their cybersecurity defenses. The Enterprise Level Security Metrics project addresses this challenge by developing practical and useful decision aids and techniques that enable organizations to better gauge and measure their security posture and help users make informed decisions based on threats and cost. **Website: U.S. Department of Homeland Security Science and Technology Enterprise Level Security Metrics and Usability**

Modeling of Internet Attacks

The growth in the complexity of network systems continues to introduce new and larger attack surfaces that can be exploited by malicious actors. The multi-faceted Internet Measurement and Attack Modeling (IMAM) Modeling of Internet Attacks project is discovering and modeling the ways malicious actors infiltrate systems and how to close the attack surface by identifying, preventing and mitigating attacks during the three phases of the attack cycle: before an attack starts, as an attack is unfolding, and during the post-attack period.

Website: U.S. Department of Homeland Security Science and Technology Internet Measurement and Attack Modeling

Moving Target Defense

Information technology (IT) systems operate in a relatively static configuration on hardware that is presumed to be safe and trusted. However, static systems provide a substantial advantage to attackers that enables them to observe the operation of key IT systems. The Moving Target Defense (MTD) project is seeking to develop game-changing capabilities that continually modify attack surfaces—thereby making it more difficult for attackers to exploit and attack—and technologies that enable systems to continue to function and meet mission needs while a cyberattack is occurring.

Website: U.S. Department of Homeland Security Science and Technology Moving Target Defense

Network Mapping and Measurement

The constantly changing nature of the Internet necessitates that researchers understand the Internet's foundational elements to improve the experiences of users, reduce the cost of measuring the Internet, and protect the nation's cyber infrastructure. The IMAM Network Mapping and Measurement project provides data to researchers about the current state of the Internet, shows how outages affect users, and what solutions will improve network reliability.

Website: U.S. Department of Homeland Security Science and Technology Internet Measurement and Attack Modeling

Resilient Systems and Networks

Detection and mitigation efforts are often performed after an attack already has occurred due to several factors, including constantly evolving attack tactics and networks that are unable to detect threats and block attacks as they occur. The IMAM Resilient Systems and Networks project is developing technologies such as real-time protocol analysis that can identify and alert when network attacks are occurring. These solutions will enable systems to be more resilient to attacks and more easily recover from an attack.

Website: U.S. Department of Homeland Security Science and Technology Internet Measurement and Attack Modeling

Security of Cloud-Based Systems

Cloud computing has changed the way organizations deploy and manage IT assets. However, the transition to the cloud has introduced new vulnerabilities and attack methods. To address these challenges, the Security of Cloud-Based Systems project is developing technologies that will help mitigate the security implications of cloud computing.

Website: U.S. Department of Homeland Security Science and Technology Security of Cloud -Based Systems

Open-Source Technologies

Homeland Open Security Technology

Despite the rapid increase in cybersecurity threats to the nation, the government's IT infrastructure is expansive and often slow to adapt and transitioning cybersecurity innovation from government research to the marketplace remains challenging. To address these complex issues, the Homeland Open Security Technology project is increasing awareness of open-security methods, models and technologies that provide sustainable approaches to support national cybersecurity objectives.

Website: U.S. Department of Homeland Security Science and Technology Homeland Open Security Technology

Secure Protocols

Secure Protocols for the Routing Infrastructure

Routing infrastructure is one of the most critical components of the Internet, yet it is susceptible to spoo ing and other attacks in which cyber criminals can redirect users to unsafe websites or pathways. The Secure Protocols for the Routing Infrastructure project's goal is to add security to the Internet's core routing protocol, namely Border Gateway Protocol (BGP), so communications follow the intended path between organizations.

Websites: U.S. Department of Homeland Security Science and Technology Secure Protocols

Open Source Suite for RPKI: rpki.net

Open Source Relying Party Software: GitHub

Software Assurance

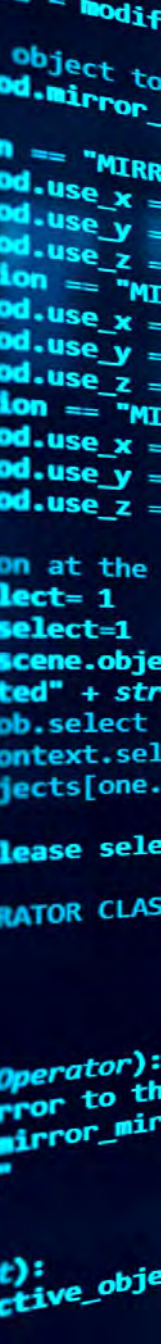
Application Security Threat and Attack Modeling

Software is ubiquitous; it powers our critical infrastructure as well as our personal lives. With the increasing number of attacks targeting poorly developed software systems, there is a need to address security early and throughout the software development process. The Application Security Threat and Attack Modeling (ASTAM) project brings together contexts from application security testing tools, automates application security testing, and provides continuous monitoring capabilities to monitor application security controls. The goal of the ASTAM project is to create a Unified Threat Management (UTM) system that enables cybersecurity professionals to monitor and analyze software systems and applications so they can more easily identify potential risks like security threats and exposures to the system environment. The system then develops appropriate countermeasures to prevent or mitigate the effects of threats to the system environment by bringing together independent assessment activities to provide better situational awareness of potential threats.

Software Quality Assurance

The growing reliance on software makes everyone vulnerable to cyberattacks. The complexity and size of software makes it difficult for software quality assurance tools to identify potential weaknesses that expose vulnerabilities in software. The Software Quality Assurance project is working to create and improve the techniques and capabilities used in static, binary and dynamic analysis tools to help create a healthier and more secure software ecosystem.

Website: **U.S. Department of Homeland Security Science and Technology Software Quality Assurance**



Software Assurance Marketplace

Software has become an essential component of the nation's critical infrastructure. It has grown in size, capability and complexity at a rate that exceeds our ability to keep pace with quality software. The Software Assurance Marketplace (SWAMP) is S&T's response to address the growing concern. This project provides a broad range of software assurance services and capabilities to help improve the quality and security of software as well as improve the overall capabilities in software quality assurance tools. SWAMP helps to formalize software assurance in organizations and provides a collaborative research environment for tool developers and researchers to advance software assurance capabilities. This national-level resource will change the software assurance community for years to come.

Websites: **U.S. Department of Homeland Security Science and Technology Software Assurance Marketplace**

SWAMP: **Software Assurance Marketplace**

Static Tool Analysis Modernization Project

The Static Tool Analysis Modernization Project (STAMP) project is a revolutionary approach to modernizing and advancing the capabilities of static analysis tools. STAMP's goal is to improve tool coverage and seamlessly integrate it into the software delivery pipeline to achieve "security at speed" in the software development process. STAMP focuses on closing the gaps in two key areas: R&D and implementation of new techniques for static software analysis. It also is working to apply new and improved testing and evaluation capabilities so static analysis continuously evolves and thereby keeps pace with modern software.


CYBERSECURITY
R&D
TRANSITION
MARKET-
PLACE

Transition

Transition to Practice

Transitioning new technologies out of the research laboratory and into the commercial marketplace can be a difficult task. The Transition to Practice (TTP) program accelerates the transition of cybersecurity research into widespread deployment. It identifies technologies developed with government funding at federal laboratories or academic institutions that have a high probability of successful transition and would have notable impact on the nation's cybersecurity posture. The TTP program accomplishes its mission by developing partnerships and serving as a connection point between the federal research community, network operators and private industry.

Website: U.S. Department of Homeland Security Science and Technology Transition to Practice

The DHS Silicon Valley Innovation Program

In late 2015, DHS established a Silicon Valley Innovation Program (SVIP), with the goal to strengthen critical relationships and engage entrepreneurs and innovators from small startups to large companies, incubators and accelerators. The SVIP, led by DHS S&T, seeks to tap into the innovation of the private sector in new ways, making it easier for technology startups to work with the government as a customer for their solutions. The SVIP's approach is to explain the challenges and operational constraints faced by the nation and the Homeland Security Enterprise and empower innovators to use their full creativity to propose and develop solutions.

In December 2015, the SVIP released the Innovation Other Transaction Solicitation (OTS), a simplified contractual authority targeting startups with a streamlined application process, fast-track selection timelines, expedited fund transfers, rapid operator feedback, and no dilution of ownership. The SVIP is seeking solutions to challenges that range across the entire spectrum of

the homeland security mission. It has issued several OTS calls on a variety of topics, including Internet of Things Security, Small Unmanned Aircraft Systems Capabilities, Enhancing Customs and Border Protection Airport Passenger Processing, K9 Wearable Technologies, Enhancements to the Global Travel Assessments System, and Financial Services Cyber Security Active Defense. Additional calls describing specific new technical areas and use cases will be issued under the Innovation OTS in the future.

Website: U.S. Department of Homeland Security Science and Technology DHS S&T's Homeland Security Innovation Programs

ONLINE
U.S. Department of
Homeland Security Cyber
Security Division

EMAIL
SandT-Cyber-Liaison@hq.dhs.gov

TWITTER
@dhsscitech

FACEBOOK
Facebook.com/dhsscitech

YOUTUBE
DHS Science and
Technology Directorate

PERISCOPE
@dhsscitech