CYBER SECURITY DIVISION

2018 PORTFOLIO GUIDE

Homeland Security

Science and Technology


SECURING
YOUR
CYBER
FUTURE

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. This comprehensive approach is aligned with several federal strategic plans, including the Federal Cybersecurity Research and Development Strategic Plan announced in February 2016, National Critical Infrastructure Security and Resilience Research and Development Plan released in November 2015 and the National Privacy Research Strategy unveiled in June 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 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: www.dhs.gov/cyber-research

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.GOV

The need for federal government departments and agencies to have a strong security posture is poignantly clear. CSD is working closely with federal civilian departments and agencies, the DHS National Protection and Programs Directorate and industry to develop and transfer modern and advanced prototyped cybersecurity capabilities. Cyber.gov is a multi-tiered, applied R&D effort to create a robust, innovative and holistic cybersecurity architecture design that mitigates modern and emerging threats by leveraging best practices—to include fine-grained monitoring and control, whitelist-based security policies, automated cybersecurity decision loop and continuous risk analysis—with minimal impact to workforce IT efficiency. The program will characterize current and evolving threats to help drive system requirements, to include technology considerations protecting cloud and mobile services, thereby ensuring newly developed or integrated cyber defense capabilities are relevant and effective against those threats. Ultimately, this approach will result in actionable guidance and implementable technology that will aid chief information officers and chief information security officers in securing their department and agencies.

CYBER FOR CRITICAL INFRASTRUCTURE

CRITICAL INFRASTRUCTURE DESIGN AND ADAPTIVE RESILIENT SYSTEMS

The Critical Infrastructure Design and Adaptive Resilient Systems (CIDARS) 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 to facilitate the development and implementation of integrated solutions that will enable secure and resilient service provisioning.

Website: www.dhs.gov/science-and-technology/csd-CIDARS

THE CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE: A DHS CENTER OF EXCELLENCE

The DHS S&T 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 to conduct research and education to enhance the resilience of the nation's critical infrastructure, 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: www.ciri.illinois.edu | www.hsuniversityprograms.org

CYBERSECURITY FOR ENERGY SYSTEMS

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: https://cred-c.org

CYBERSECURITY FOR OIL AND GAS SECTOR

The Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) project is an ongoing collaboration between CSD, oil and natural gas companies. The collaborative project was formed in 2004 to facilitate cooperative research, development, testing and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. The project undertakes collaborative R&D projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector. The project objective is to promote the interests of the sector while maintaining impartiality, the independence of the participants and vendor neutrality. After a successful first project, the LOGIIC consortium was formally established as a collaboration between DHS, the Automation Federation, and five of the major oil and gas companies.

Website: www.dhs.gov/science-and-technology/csd-COGS

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: www.dhs.gov/science-and-technology/csd-cpssec

CYBER-ENABLED NETWORKED PHYSICAL SYSTEMS

CPS and IoT are designed with computation and communication, including machine-to-machine communication capabilities. This design has resulted in new cybersecurity challenges and the risks only increase as CPS and IoT systems are scaled and designed to work in autonomous situations. This applied research will address issues in security, trust, context-awareness, ambient intelligence and reliability.

Website: www.dhs.gov/science-and-technology/csd-cpssec

INTERNET OF THINGS SECURITY

The internet of things (IoT) continues to emerge and expand as costs drop and the confluence of sensors, platforms and networks increases. The deployment and adoption of IoT devices and systems can provide vast opportunities for DHS and Homeland Security Enterprise (HSE) missions while simultaneously increasing cybersecurity risks and expanding attack surfaces for adversaries. The consequences of an incident—unintentional or malicious—could result in cascading impacts affecting both critical infrastructure and human lives. Internet of Things Security (IoTSEC) is an applied R&D project that addresses the gaps between high-order frameworks and emerging classes of IoT cybersecurity capabilities and products maturing and becoming available. This project will provide mission operators, enterprise chief information and information security officers a realistic architectural roadmap and design pattern with a proof-of-concept demonstration. Outcomes will improve the understanding and confidence of organizations to more rapidly insert and deploy IoT security capabilities to match IoT sensors, actuators, communications, computing and mission demands.

Website: www.dhs.gov/science-and-technology/csd-cpssec

CYBERSECURITY FOR LAW ENFORCEMENT

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: www.dhs.gov/CSD-ANC

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: www.dhs.gov/science-and-technology/csd-forensics

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: www.dhs.gov/science-and-technology/csd-competitions
Competitions: http://nccdc.org/ | www.uscyberchallenge.org/

CYBERSECURITY RESEARCH INFRASTRUCTURE

EXPERIMENTAL RESEARCH TESTBED

It is important that new cybersecurity approaches are evaluated in a realistic environment. The Experimental Research Testbed, also known as the Defense Technology Experimental Research (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: www.dhs.gov/science-and-technology/csd-deter | www.deter-project.org/

INFORMATION MARKETPLACE FOR POLICY AND ANALYSIS OF CYBER-RISK & TRUST

The Information Marketplace for Policy and Analysis of Cyber-risk & Trust (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: www.dhs.gov/csd-impact | www.impactcybertrust.org/

HOMELAND OPEN SECURITY TECHNOLOGY

HOMELAND OPEN SECURITY TECHNOLOGY

The Homeland Open Security Technology (HOST) project is gathering information from state and local governments about their consideration and implementation of open-source cybersecurity solutions. The project will use the insight and experiences collected to develop best practices for adoption of open-source solutions and a lessons-learned report. The analysis also will help inform Federal R&D efforts to leverage open-source software for intergovernmental solutions that benefit the broader HSE.

Website: www.dhs.gov/science-and-technology/csd-host

HUMAN ASPECTS OF CYBERSECURITY

CYBER RISK ECONOMICS

Despite the growing focus on cybersecurity, there has been little coordination between R&D on the economics of cybersecurity and the capability gaps of the HSE. The Cyber Risk Economics (CyRiE) project addresses this gap by engaging the behavioral, technical, legal and business aspects of the economics of cyber-threats, vulnerabilities and controls. CyRiE R&D emphasizes empirically based measurement, modeling and evaluation of:

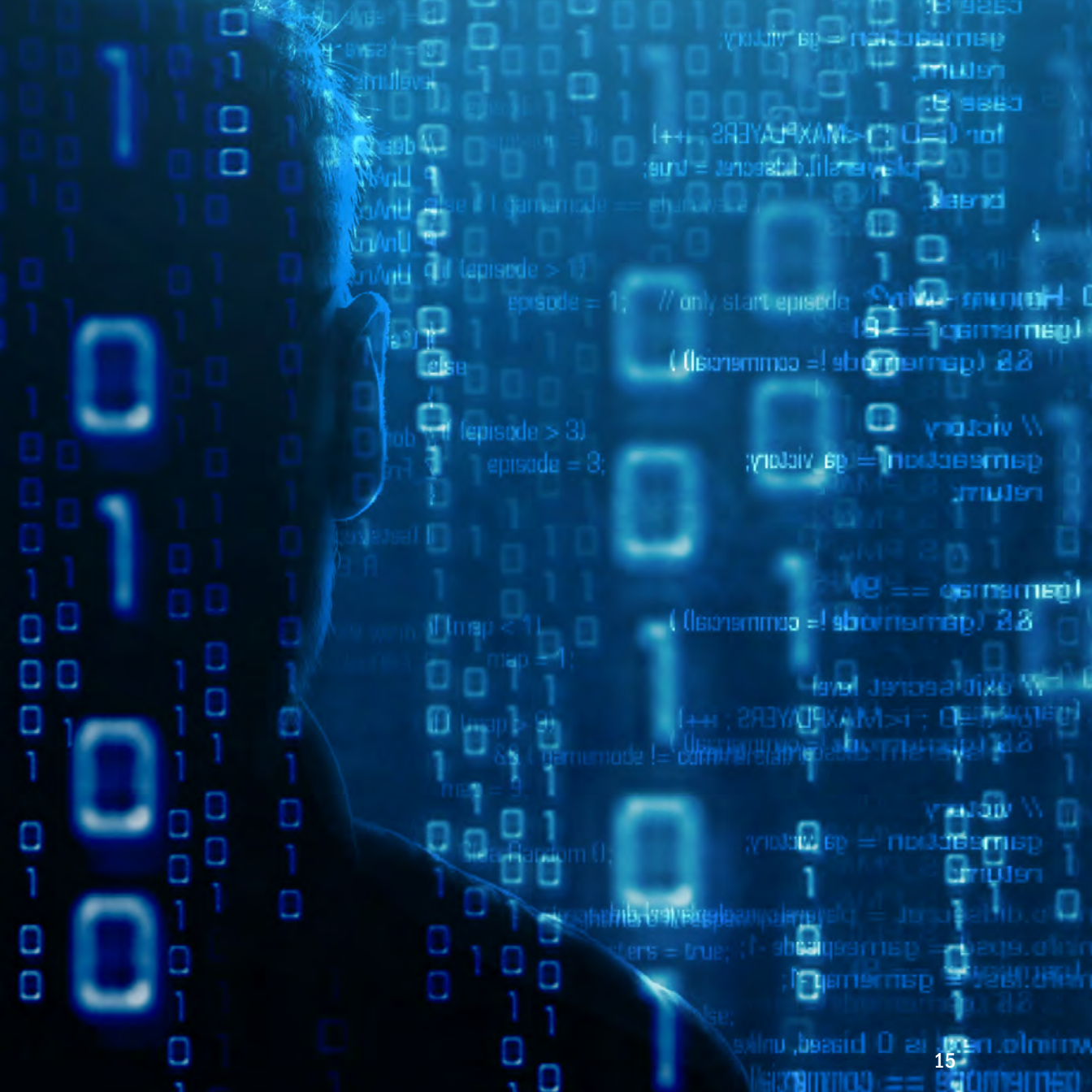
- Investment in cybersecurity controls by the private sector, government and private actors
- Impact of investment on the probability, severity and consequences of actual risks and resulting cost and harm
- Value the correlation between business performance measures and evaluations of cybersecurity investments and impacts
- Incentives to optimize the investments, impacts and value basis of cyber-risk management

Website: www.dhs.gov/science-and-technology/csd-cyrie

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: www.dhs.gov/science-and-technology/csd-insider-threat



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: www.dhs.gov/science-and-technology/csd-idm

DATA PRIVACY

The Data Privacy project develops, tests and evaluates technical and knowledge solutions for the management of privacy threats and vulnerabilities that arise from social and technical policies and operations. It focuses on privacy risks related to connected sensor devices, automated and autonomous systems, and the provisioning of digital services. The R&D objective is to better align technology capabilities with individual and social expectations of privacy.

Website: www.dhs.gov/science-and-technology/csd-privacy

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., personally identifiable information). 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: www.dhs.gov/science-and-technology/csd-mobile-app-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: www.dhs.gov/science-and-technology/csd-mobile-device-security

NETWORK SYSTEM SECURITY

APPLICATION OF NETWORK MEASUREMENT SCIENCE

Internet attacks on availability ramp up over seconds or minutes and the only viable defense many organizations have is to rely on agile response teams and other intrusion-response capabilities to manually triage the event. The Application of Network Measurement Science project will develop innovative technologies to provide a system to identify, classify, report, predict, provide attribution, and potentially mitigate Network/Internet Disruptive Events (NIDEs) that cause a material loss or degradation of service, a material reduction in resilience, or manipulation of traffic flows with adverse consequences. The Small Enterprise Assistance for Cyber (SEAC, pronounced seek) effort will develop a cost-efficient delivery system for small enterprises to improve the protection of their cyber footprint. The NIDE results will be combined with other tools and information, some of which have been developed by CSD's Internet Measurement and Attack Modeling project, to provide access to cutting-edge tools and expertise in as near real-time as possible.

Website: www.dhs.gov/science-and-technology/csd-ANMS

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 (DDoSD) 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: www.dhs.gov/science-and-technology/csd-ddosd

FEDERATED SECURITY

The security of networked systems and critical infrastructure is perhaps the biggest challenge we currently face as a nation. All aspects of society—from the consumer with a small home network to a corporate enterprise with thousands of endpoints and nodes—are affected by network security whether or not they realize it. However, the traditional concept of "isolated" networks relying on perimeter defenses such as firewalls and other standalone defense-in-depth solutions to provide the majority of a network's defenses must evolve into one in which networks are "federated." This project is developing prototypes for federated networks that will preserve member diversity, are more resilient, have active defenses to address the inevitable adversarial penetration and unauthorized access, automatically share information with other members, and contain command and control to act on information received from inside or outside sources, effectively enabling local decision-making based on global knowledge.

Website: www.dhs.gov/science-and-technology/csd-federated-security

NEXT GENERATION CYBER INFRASTRUCTURE APEX PROGRAM

The Next Generation Cyber Infrastructure Apex (NGCI Apex) program addresses the cybersecurity challenges facing our nation's critical infrastructure. NGCI Apex finds, tests and transfers proven solutions to these sectors to fill cybersecurity gaps and harden critical systems and networks.

Currently, NGCI Apex is working to harden the cyber-defenses of the financial services sector (FSS), which is a frequent target of cybercriminals. The Cyber Apex Review Team (CART), sponsored by CSD and made up of FSS institution and Treasury Department representatives, identifies gaps and evaluates solutions. While some identified gaps are solvable by mature technology, others needed novel ideas. This finding led NGCI Apex to establish two development paths: creating a consortium to test existing solutions and partnering with the DHS Silicon Valley Innovation Program (SVIP) for early-stage solutions.

The consortium focuses on operational testing of mature technologies to determine if they meet FSS needs. The program uses a consortium manager—Cyber Apex Solutions—to maintain an efficient process for foraging and building a consortium of technology owners.

SVIP focuses on finding novel solutions from startups whose technologies are not mature enough for rigorous operational testing and evaluation. Solutions with promise are piloted and evaluated. NGCI Apex solicitations under SVIP—the Financial Services Cyber Security Active Defense—seeks startups that have novel solutions in the areas of moving-target defense, isolation and containment and cyber-intrusion deception. Several performers have been selected.

Website: www.dhs.gov/science-and-technology/apex-ngci

SMART CITIES

CSD is working closely with National Institute of Standards and Technology (NIST) on NIST's 2017-2018 Global Cities Team Challenge (GCTC) to raise awareness of the need for cybersecurity in emerging "smart cities." The new DHS S&T-NIST "Smart and Secure Cities and Communities Challenge" (SC3) is encouraging GCTC participants to adopt designed-in cybersecurity for "smart city" systems that are more secure, reliable, resilient and protective of privacy. Through SC3, CSD is promoting the development, adoption and implementation of cybersecurity protections within smart-city environments and helping DHS S&T-funded programs and performers bring their solutions into the GCTC.

CSD is also calling on innovators from the cybersecurity industry and research community to teach cities, communities and GCTC teams about cyber challenges, cyber physical systems and internet-of-things devices to help address cybersecurity and privacy objectives.

Website: www.dhs.gov/science-and-technology/csd-smart-cities

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.

Website: www.dhs.gov/science-and-technology/csd-ASTAM

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: www.dhs.gov/science-and-technology/csd-sqa

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: www.dhs.gov/science-and-technology/csd-swamp
https://continuousassurance.org/

STATIC TOOL ANALYSIS MODERNIZATION PROJECT

The Static Tool Analysis Modernization Project (STAMP) 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.

Website: www.dhs.gov/science-and-technology/csd-STAMP

TRANSITION TO PRACTICE

ACCELERATING TECHNOLOGY TRANSITION

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: www.dhs.gov/science-and-technology/csd-ttp


TTP
CYBERSECURITY R&D
MARKETPLACE

THE DHS SILICON VALLEY INNOVATION PROGRAM

The DHS S&T Silicon Valley Innovation Program (SVIP) is keeping pace with the innovation community to tackle the hardest problems faced by DHS's operational missions and the Homeland Enterprise System. SVIP is expanding DHS S&T's reach to find new technologies that strengthen national security, with the goal of reshaping how government, entrepreneurs and industry work together to find cutting-edge solutions. SVIP, based in California's Silicon Valley, connects with innovation communities across the nation and around the world to harness the commercial R&D ecosystem for government applications, co-invest in ideas, and accelerate transition-to-market.

Through a streamlined application and pitch process, SVIP is seeking solutions to challenges that range across the entire spectrum of the homeland security mission, including cybersecurity and technology solutions for Customs and Border Protection and first responders. SVIP can award a maximum of $800,000 (up to $200,000 per phase) across four phases spanning a 24-month period.

Since launching in December 2015, the SVIP has:

- Received more than 250 applications
- Made awards to more than 25 companies
- Leveraged more than $400 million in private-sector investments

For more information, visit scitech.dhs.gov/hsip or send an email to: DHS-Silicon-Valley@hq.dhs.gov.

ONLINE
www.dhs.gov/cyber-research

FACEBOOK
Facebook.com/dhsscitech

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

YOUTUBE
www.youtube.com/dhsscitech

TWITTER
@dhsscitech

PERISCOPE
@dhsscitech

LINKEDIN
dhsscitech