Homeland Security

Science and Technology

2016 I Cyber Security Division

R&D SHOWCASE AND TECHNICAL WORKSHOP

February 17–19, 2016

SECURING YOUR CYBER FUTURE

WHAT'S NEW

Silicon Valley Office

S&T CSD is now leading the Department's new Silicon Valley Office (SVO) to bring some of the toughest homeland security challenges to our nation's innovation community. The SVO will engage non-traditional performers, such as start-ups and incubators, to help them consider DHS as a viable customer for their technology.

Next Generation Cyber Infrastructure APEX

Launched in 2015, the Next Generation Cyber Infrastructure (NGCI) Apex Program addresses primary functional gaps for the financial services sector by providing tools and technologies—many from CSD's portfolio—to combat advanced adversaries and protect U.S. cyber systems and networks.

WELCOME

Douglas Maughan, Ph.D.

Cyber Security Division Director

Welcome to the 2016 Cyber Security Division (CSD) Research and Development (R&D) Showcase and Technical Workshop. After engaging more than 550 cybersecurity professionals last year, the CSD—within the Homeland Security Advanced Research Projects Agency (HSARPA) of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T)—has continued to expand our footprint with innovative research in close collaboration with the DHS operators, other federal agencies, industry, and our international partners. Together we have demonstrated technologies that will help improve the cybersecurity landscape.

Today's R&D Showcase features nine innovative, transition-ready solutions and two collaboration projects with the private sector selected from our portfolio that address a variety of complex challenges, from mobile and cyber physical systems security to software assurance. From 3:30 - 6:00pm, join us for the technology demonstration and poster session to engage with our funded performers. The two-day Technical Workshop will feature over 70 presentations, highlighting the work of CSD's Principal Investigators. Throughout the event, we want to provide each of you the opportunity to experience our entire portfolio and actively engage with our funded researchers.

As you participate in the Showcase and Technical Workshop, I encourage you to think about S&T CSD, the research and technologies, and the opportunities where you can bring these solutions into your operational environments to help improve our nation's cybersecurity posture. I also recommend that you engage with the CSD Program Managers and staff on new areas for R&D.

Since 2003, CSD has actively engaged the public and private sector, the National Labs and our international partners to develop innovative cybersecurity solutions. We are pleased to have all of you with us over the next three days and thank you for your support of the DHS S&T CSD program and mission. With each year, it becomes even more evident that cybersecurity R&D continues to be a global team sport.

Cyber Security Division Director
Department of Homeland Security
Science and Technology Directorate

“Our nation is facing many complex cybersecurity challenges. S&T’s cyber team is leveraging global talent through international partnerships, university center of excellences, national laboratories, and private sector firms to develop solutions to hard complex problems.”

Dr. Reginald Brothers
DHS Under Secretary for Science and Technology

CONTENTS

SCIENCE AND TECHNOLOGY DIRECTORATE

Mission

Established by Congress in 2003, S&T's mission is to deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise (HSE). As DHS's primary R&D arm, S&T manages science and technology research, from development through transition, for the department's operational components and the nation's first responders. S&T's engineers, scientists and researchers work closely with industry and academic partners to ensure R&D investments address the high-priority needs of today and the growing demands of the future.

From border security and biological defense to cybersecurity and explosives detection, S&T is at the forefront of integrating R&D across the public and private sectors and the international community. By working directly with responders and component partners across the nation, S&T strives to provide advanced capabilities and analytics to better prevent, respond to and recover from all hazards and homeland security threats.

Focus Areas

S&T works with the broader R&D community to identify and adapt existing R&D investments to meet operator needs and challenges in four general areas:

- S&T creates technological capabilities that address DHS operational and strategic needs or that are necessary to address evolving homeland security threats.
- S&T conducts systems-based analysis to provide streamlined, resource-saving process improvements and efficiencies to existing operations.
- DHS achieves more effective and efficient operations and avoids costly acquisition failures and delays by leveraging S&T's technical expertise to improve project management, operational analysis and acquisition management.
- S&T's relationships across DHS and the HSE contribute to the strategic understanding of existing and emerging threats and recognition of opportunities for collaboration across departmental, interagency, state and local and international boundaries.

Partnerships across the diverse R&D landscape—federal, state, local, tribal and territorial agencies; private industry; and academia—are the foundation for S&T's successful technology foraging efforts and adaptation of existing R&D investments to homeland security mission needs. S&T's understanding of the ever-changing threat environment and our relationships with the men and women who combat those threats every day make the organization an effective catalyst for improving the security and resilience of our nation.

Homeland Security

Science and Technology

DHS S&T Cyber Security Division

Securing YOUR Cyber Future

Our Mission is to:

DEVELOP & DELIVER

Develop and deliver new technologies, tools, and techniques to enable customers to defend, mitigate, and secure current and future systems, networks, and critical infrastructure against cyber attacks.

TRANSITION

Conduct and support technology transition and approaches across the HSE by identifying mature technologies that address existing or imminent cybersecurity gaps.

LEAD & COORDINATE

Lead and coordinate research and development among DHS components and customers, other government agencies, academia, private sector, and international partners within the cybersecurity community.

DHS S&T Cyber Security Division Website

DHS S&T Cyber Security Division Email address

DHS S&T Cyber Security Division Twitter page

DHS S&T Cyber Security Division Facebook page

DHS S&T Cyber Security Division YouTube page

SILICON VALLEY OFFICE

In April 2015, Secretary of Homeland Security Jeh Johnson announced plans to open up a satellite office in Silicon Valley to strengthen critical relationships and engage entrepreneurs and innovators from small startups to large companies, incubators, and accelerators. The SVO seeks to tap into the innovation of the private sector in new ways, opening the doors for non-traditional performers to work with government and to consider the government as a viable customer for their technology.

While traditional government contracting tends to dictate exactly how to do things, DHS recognizes that innovators do not work in that way. The SVO's approach will be to explain the challenges and operational constraints faced by the nation and the HSE and allow them to use their full creativity to develop solutions.

The DHS SVO will build on the work the Science and Technology Directorate's (S&T) Cyber Security Division has been doing over the last decade. During this time, S&T has funded more than 40 cybersecurity technical areas with over $400 million in funding with strong bipartisan Congressional support.

Led by S&T and CSD, the SVO will focus on outreach throughout FY 2016 to cultivate relationships with the innovation community in the Silicon Valley as well as other innovation corridors around the country. The SVO will conduct ideation workshops to identify solutions addressing both commercial and government applications. Informed by these workshops, S&T intends to co-fund innovative research, facilitate demonstrations and pilots, and accelerate transition into use by DHS and other users in the HSE by FY 2017.

In December 2015, the SVO released the Innovation Other Transaction Solicitation (OTS) (**Federal Business Opportunities website**) aimed at startups, providing a streamlined application process, fast-track selection timelines, expedited fund transfers, rapid operator feedback, and no dilution of ownership. Although DHS will be seeking solutions to challenges that could range across the entire spectrum of the homeland security mission, the first challenge is focused on security of Internet-of-Things.

HOMELAND SECURITY

#STARTUPDHS

ENGAGING INNOVATION CORRIDORS

For more information, visit the **DHS Silicon Valley website** or **email DHS Silicon Valley.**

S&T'S NEXT GENERATION CYBER INFRASTRUCTURE APEX PROGRAM

Protecting the Nation's Cyber Infrastructure

Cyber attacks threaten national security by undermining information-dependent critical infrastructure. DHS identified 16 critical infrastructure sectors designated in the Presidential Policy Directive (PPD-21) - Critical Infrastructure Security and Resilience. Subsequently, DHS S&T Directorate's CSD and the financial services sector identified three major challenges to securing the financial sector's networks:

- Adversaries are infiltrating our systems and networks without our knowledge.
- The sectors' understanding of the cyber situation is inaccurate, incomplete, or only achieved forensically and after the infiltration has occurred.
- Network owners/operators lack strong ways to respond and mitigate the impact of adversaries on our systems and still allow the sector to maintain adequate operating capacity

Apex NGCI Program

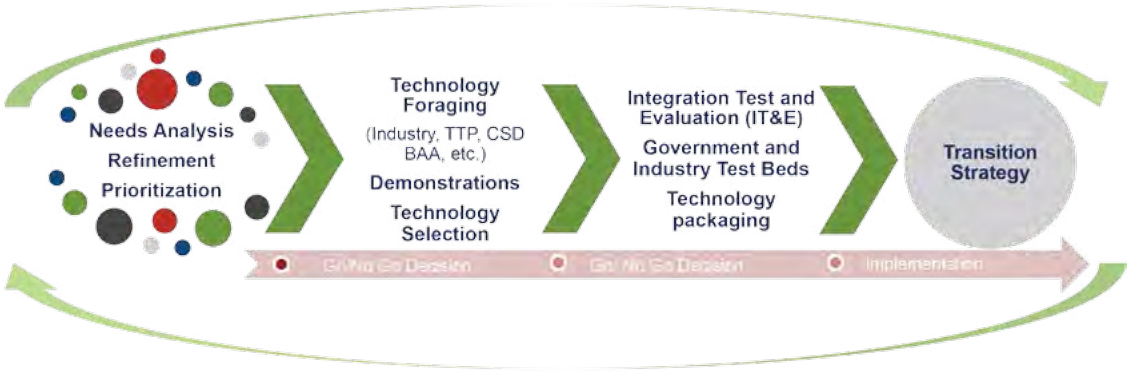
The NGCI Apex Program addresses these challenges by providing the financial services sector with the technologies and tools to confront advanced adversaries when they attack U.S. cyber systems and networks.

NGCI will concentrate on delivering capabilities identified by the financial sector to address five primary functional gaps: (1) Dynamic Defense, (2) Network Characterization, (3) Malware Detection, (4) Software Assurance and (5) Insider Threat.

Customer and Stakeholder Engagement

- Done in collaboration with the Department of Treasury and financial service sector, NGCI evaluates tools that can help defend against threats.
- Working with sector chief information security officers, NGCI has established the Cyber Apex Review Team (CART) to define prioritized requirements, plan and execute test and evaluation activities, and carry out the most appropriate methods of technology deployment and transition.

NGCI uses a repeatable, continuous process to identify, test, evaluate and transition cyber technologies to the Financial Services Sector



“Cybersecurity is only as strong as our weakest link. S&T is actively engaging our international partners to improve our systems and networks. The more we can work with our allies to ensure that their infrastructure is secure, the more secure we all will be.”

Dr. Douglas Maughan
Cyber Security Division Director, DHS S&T

AGENDA

February 17, 2016

7:15am - 8:15am	REGISTRATION
	GENERAL SESSION
8:15am - 8:30am	**Introductions/Welcome | Douglas Maughan,** DHS S&T CSD Division Director
8:30am - 9:10am	**Keynote**
9:10am - 9:40am	**CSD Strategic Vision | Douglas Maughan,** DHS S&T CSD Division Director
9:40am - 10:20am	**R&D In Operational Environments Panel |** ***Moderator:*** **Scott Tousley,** DHS S&T CSD Deputy Director; ***Panelists:*** **Ann Barron DiCamillo,** Director, United States Computer Emergency Readiness Team (US-CERT), DHS, Office of Cybersecurity and Communications; **James Darnell,** Special Agent in Charge (ATSAIC), United States Secret Service (USSS); **Michael Hamilton,** Lead Security Consultant, Critical Informatics; **Robert Kaminski,** Senior Electronics Engineer, Information Directorate, Air Force Research Laboratory
10:20am -10:35am	MORNING BREAK
10:35am - 12:15pm	**CSD SHOWCASE**
10:35am - 10:55am	**Situ: Discovering Suspicious Behavior in Cyber Security** **John Goodall,** Oak Ridge National Laboratory
10:55am - 11:15am	**A Watchdog System for Internet Routing** **Christos Papadopoulos,** Colorado State University
11:15am - 11:35am	**Towards a Global Network Reputation System: A Mechanism Design Approach** **Mingyan Liu,** University of Michigan
11:35am - 11:55am	**Federated Command and Control for Adaptive Computer Network Security** **Marco Carvalho,** Florida Institute of Technology
11:55am - 12:15pm	**Accelerating the Discover, Identification, and Remediation of Application Vulnerabilities with Hybrid Analysis Mapping** **Dan Cornell,** Denim Group
12:15pm - 1:15pm	**LUNCH (on own)**
1:15pm - 3:15pm	**CSD SHOWCASE**
1:15pm - 1:35pm	**MobileRoT: A Fully Software-based Mobile Security Architecture** **Kris Carver,** BlueRISC
1:35pm - 1:55pm	**Project iVe: Forensics for Vehicle Infotainment and Navigation Systems** **Ben LeMere,** Berla Corporation
1:55pm - 2:15pm	**Protecting Emergency Services from Complex Distributed Telephone Denial of Service** **Mark Collier,** SecureLogix
2:15pm - 2:35pm	**DHS IMPACT: Datasets for Use in Cyberesecurity Research** **Paul Royal,** Georgia Tech Information Security Center
2:35pm - 2:55pm	**Linking the Oil and Gas Industry to Improve Cybersecurity: Collaborative Research Within the Oil and Natural Gas Industry** **Barry Cott,** Shell
2:55pm - 3:15pm	**Cyber Apex: Next Generation Cyber Infrastructure** **Eric Harder,** DHS S&T CSD
3:15pm - 3:30pm	**AFTERNOON BREAK**
3:30pm - 6:00pm	**TECHNOLOGY DEMONSTRATION / POSTER SESSION**

AGENDA

February 18, 2016

7:30am - 8:30am	REGISTRATION
	GENERAL SESSION
8:30am - 8:40am	**Introductions/Welcome** | **Douglas Maughan,** DHS S&T CSD Division Director
8:40am - 9:10am	**Keynote**
9:10am - 10:10am	**Technology Transition Success Panel** | *Moderator:* **Mike Pozmantier,** DHS S&T CSD *Panelists:* **Jake Braun,** Cambridge Global; **Stan Brown,** Ernst & Young LLP; **Nicholas Chaillan,** Cyber Revolution; **Andrew Hoog,** NowSecure; **Joshua Neil,** Security Analytics; **Salvatore Stolfo,** Red Balloon Security
10:10am - 10:30am	**International Special Speaker** | **Andy Williams,** United Kingdom (UK) Cyber Envoy, UK Trade and Industry Defence and Security Organization

○ EARLY ◉ MID ● MATURE

TRACK 1

10:45am - 10:50am	**CYBER SECURITY INCIDENT RESPONSE TEAM (CSIRT)** | PM Introduction: Scott Tousley
10:50am - 11:10am	**CSIRT Findings and Transition** | **Reeshad Dalal,** Dartmouth College
11:10am - 11:15am	**ANONYMOUS NETWORKS & CURRENCIES** | PM Introduction: Megan Mahle
11:15am - 11:25am	**Illuminating Onions** | **Rob Jansen,** Naval Research Lab
11:25am - 11:35am	**New Frontiers in Illicit Commerce: Bitcoin and Law Enforcement** | **Andrew Cox,** Sandia National Lab
11:35am - 11:45am	**Anonymous Networks and Currencies: New Award**
11:45am - 11:50am	**CYBER FORENSICS** | PM Introduction: Megan Mahle
11:50am - 12:10pm	**Project iVe: Vehicle Infotainment and Navigation System Forensics** | **Brian Carrier,** Basis Technology
12:10pm - 1:15pm	**LUNCH (on own)**
1:15pm - 1:35pm	**NIST Tool Testing & Software Dataset** | **Barbara Guttman,** National Institute of Standards and Technology
1:35pm - 1:40pm	**SECURITY FOR CLOUD-BASED SYSTEMS** | PM Introduction: Edward Rhyne
1:40pm - 2:00pm	**Silverline: Assessment System for Secure Cloud Computing** | **Rob Joyce,** ATC-NY
2:00pm - 2:20pm	**CloudCOP: Secure and Resilient Self-Healing Cloud** | **Aleksey Nogin,** HRL Laboratories
2:20pm - 2:35pm	**The CipherRack Secure Cloud** | **Radu Sion,** Private Machines
2:35pm - 2:45pm	AFTERNOON BREAK
2:45pm - 2:50pm	**MOVING TARGET DEFENSE** | PM Introduction: Edward Rhyne
2:50pm - 3:10pm	**Building a Moving Target Reference Implementation** | **Andrew Mellinger,** Carnegie Mellon University Software Engineering Institute
3:10pm - 3:30pm	**Hardware Support for Malware Defense and End-to-End Trust** | **Dimitrios Pendarakis,** IBM
3:30pm - 3:50pm	**Hardware-Enabled Zero Day Protection** | **Omar Quimbaya,** Def-Logix
3:50pm - 3:55pm	**HOMELAND OPEN SECURITY TECHNOLOGY** | PM Introduction: Daniel Massey
3:55pm - 4:05pm	**Interagency Open Technology Transfer** | **John Weathersby,** Open Technology Center
4:05pm - 4:15pm	TRANSITION BREAK

TRACK 2

○ EARLY ◉ MID ● MATURE

10:45am - 10:50am	**SOFTWARE QUALITY ASSURANCE | PM Introduction: Kevin Greene**
10:50am - 11:10am	**Tunable Information Flow: Policy-Driven Software Assurance | Aleksey Nogin,** HRL Laboratories
11:10am - 11:30am	**Static Analysis of x86 Executables Using Abstract Interpretation | Henny Sipma,** Kestrel Technology
11:30am - 11:45am	**Hybrid Analysis Mapping | Ken Prole,** Secure Decisions
11:45am - 12:00pm	**An Architecture-centric Approach to Security Analysis | Carol Woody,** Carnegie Mellon University Software Engineering Institute
12:00pm - 12:15pm	**Detection and Family Identification of Android Malware | Sam Malek,** University of California, Irvine
12:15pm - 1:15pm	**LUNCH (on own)**
1:15pm - 1:30pm	**General Analysis Toolkit Using Record and Replay (GATOR) | Julian Grizzard,** Johns Hopkins University
1:30pm - 1:45pm	**Evaluating Static Code Analysis Tools and Reducing Their False Positives | James Hill,** Indiana University-Purdue University Indianapolis
1:45pm - 1:55pm	**Vendor Truth Serum | Greg Klass,** Ball State - Georgetown
1:55pm - 2:05pm	**Real-time Application Security Analyzer (RASAR) for Application Security | Robert McGraw,** RAM Laboratories
2:05pm - 2:10pm	**SECURE PROTOCOLS | PM Introduction: Daniel Massey**
2:10pm - 2:25pm	**Ensuring and Accelerating Routing Security (EARS) | Sandra Murphy,** Parsons Corporation
2:25pm - 2:45pm	AFTERNOON BREAK
2:45pm - 2:50pm	**DATA PRIVACY | PM Introduction: Anil John**
2:50pm - 3:00pm	**Data Privacy: New Award**
3:00pm - 3:10pm	**Data Privacy: New Award**
3:10pm - 3:20pm	**Data Privacy: New Award**
3:20pm - 3:25pm	**IDENTITY MANAGEMENT | PM Introduction: Anil John**
3:25pm - 3:35pm	**Identity Applied Research & Advance Development Projects | Fred Roberts and Robin Wilson,** Rutgers University/Kantara Initiative
3:35pm - 3:40pm	**INSIDER THREAT | PM Introduction: Megan Mahle**
3:40pm - 4:00pm	**Monitoring DBMS Activity for Detecting Data Exfiltration by Insiders | Donald Steiner,** Northrop Grumman
4:00pm - 4:15pm	TRANSITION BREAK

4:15pm - 5:30pm	**COLLABORATION SESSIONS**

TOPIC 1: "Going Dark": Technical challenges and potential solutions

TOPIC 2: Cyber Security Transition and Commercialization Pathways

TOPIC 3: Measuring Cyber Security Research and Development Impact

TOPIC 4: "Blue Sky" Session

TOPIC 5: Cyber Economic Incentives and Insurance

For more information refer to pages 30-31.

AGENDA

February 19, 2016

7:30am - 8:30am	REGISTRATION
	DUAL TECHNICAL TRACKS
8:30am - 8:35am	**Introductions/Updates** | Douglas Maughan, DHS S&T CSD Division Director and Scott Tousley, DHS S&T CSD Deputy Director

○ EARLY ◉ MID ● MATURE

TRACK 1

8:35am - 8:40am	**CYBER ECONOMICS** | PM Introduction: Joseph Kielman
8:40am - 9:00am	**Understanding and Disrupting the Economics of Cybercrime** | Nicolas Christin, Carnegie Mellon University
9:00am - 9:15am	**Increasing the Impact of Voluntary Action Against Cybercrime** | Tyler Moore, University of Tulsa
9:15am - 9:25am	**Applying Behavioral Economics to Improve Cyber Security Behaviors: A Cyber Insurance Application** | Fariborz Farahmand, Georgia Tech
9:25am - 9:30am	**MOBILE DEVICE SECURITY** | PM Introduction: Vincent Sritapan
9:30am - 9:50am	**Critical Applications for Mobile Roots of Trust** | Erin Chapman, Galois, Inc.
9:50am - 10:10am	**Physical Unclonable Functions for Mobile Device Roots of Trust** | Omar Quimbaya, Def-Logix
10:10am - 10:25am	**Mobile Application Communications Using GUI & Data Instrumentation** | Angelos Stavrou, George Mason University
10:25am - 10:35am	MORNING BREAK
10:35am - 10:50am	**Mobile Malware Analysis** | Christopher Kruegel, University of California, Santa Barbara
10:50am - 11:00am	**iSentinel: Continuous Behavior Based Authentication for Mobile Devices** | Vincent DeSapio, HRL Laboratories
11:00am - 11:10am	**Mobile App Software Assurance** | Angelos Stavrou, Kryptowire
11:10am - 11:20am	**CARAMA: Continuous Assessment of Risk Affecting Mobile Authentication** | Lap Truong, Northrop Grumman
11:20am - 11:30am	**CASTRA : A Multi-faceted Approach to User Authentication for Mobile Devices—Using Human Movement, Usage, and Location Patterns** | Devu Manikantan Shila, United Technologies Research Center
11:30am - 11:40am	**Remote Access For Mobility via Virtual Micro Security Perimeters** | Saman Aliari Zonouz, Rutgers University
11:40am - 11:50am	**Multi-Modal Mobile Security Management for User Behavior Anomaly Detection and Risk Estimation** | Ching-Yung Lin, IBM
11:50am - 12:00pm	**Theseus: A Mobile Security Management Tool for Detecting and Mitigating Attacks in Mobile Networks**| Jamie Payton, University of North Carolina at Charlotte
12:00pm - 12:10pm	**TrustMS: a Trusted Monitor and Protection for Mobile Systems** | Guang Jin, IAI Inc.
12:10pm - 12:20pm	**Continuous Authentication** | Tom Karygiannis, Kryptowire
12:20pm - 1:20pm	**LUNCH (on own)**

Track 1 continued

○ EARLY ◉ MID ● MATURE

1:20pm - 1:25pm	**CYBER PHYSICAL SYSTEMS SECURITY (CPSSEC) |** PM Introduction: Daniel Massey
1:25pm - 1:35pm	**Cyber Physical System Security for Advanced Manufacturing |** Jules White and Jaime Camelio, Virginia Tech/ Vanderbilt University
1:35pm - 1:45pm	**CPS Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments |** Manimaran Govindarasu, Iowa State University
1:45pm - 1:55pm	**Cyber Physical Attacks and Countermeasures in a Resilient Electric Power Grid |** Lalitha Sankar, Arizona State University
1:55pm - 2:05pm	**Medical Device Risk Assessment Platform |** Dale Nordenberg, Medical Device Innovation, Safety, and Security Consortium
2:05pm - 2:15pm	**Modeling Security/Safety Interactions in Buildings for Compositional Security/Safety Control** Xinming (Simon) Ou, University of South Florida
2:15pm - 2:25pm	**Secure Software Updates Over-the-Air for Ground Vehicles |** Andre Weimerskirch, University of Michigan
2:25pm - 2:35pm	**Side-Channel Causal Analysis for Design of Cyber-Physical Security |** David Payton, HRL Laboratories
2:35pm - 2:45pm	**Uptane: Securely Updating Automobiles |** Justin Cappos, New York University
2:45pm - 2:55pm	**CPS Security: New Award**
2:55pm - 3:05pm	**Automotive Cyber Security for Government Vehicles |** Kevin Harnett, Volpe
3:05pm - 3:15pm	AFTERNOON BREAK
3:15pm - 3:20pm	**ENTERPRISE LEVEL SECURITY METRICS/USABLE CYBERSECURITY** PM Introduction: Greg Wigton
3:20pm - 3:40pm	**Practical Metrics for Enterprise Security Engineering |** Bill Sanders, University of Illinois at Urbana-Champaign
3:40pm - 4:00pm	**Usable Cybersecurity |** Jean Camp, Indiana University
4:00pm - 4:10pm	AFTERNOON BREAK

	GENERAL SESSION
4:10pm - 4:30pm	**Cyber Security Division Performer Awards |** Douglas Maughan, DHS S&T CSD Division Director
4:30pm - 4:35pm	**Conference Wrap-up**

AGENDA

February 19, 2016

TRACK 2

○ EARLY ◉ MID ● MATURE

8:35am - 8:40am	**DISTRIBUTED DENIAL OF SERVICE (DDoS) DEFENSE | PM Introduction: Daniel Massey**
8:40am - 8:50am	**3DCoP: DDoS Defense for a Community of Peers | Jem Berkes,** Galois, Inc.
8:50am - 9:00am	**Black Cloud as an Anti-DDoS Solution for Cloud Applications | Juanita Koilpillai,** Waverley Labs
9:00am - 9:10am	**DrawBridge: Leveraging Software-Defined Networking for DDoS Defense** **Jun Li,** University of Oregon
9:10am - 9:20am	**NetBrane: a DDoS Protection Platform | Christos Papadopoulos,** Colorado State University
9:20am - 9:30am	**Software Systems for Surveying Spoofing Susceptibility | KC Claffy,** University of California, San Diego
9:30am - 9:40am	**SENSS: Security Service for the Internet | Jelene Mirkovic,** University of Southern California Information Sciences Institute
9:40am - 9:50am	**Ensuring Energy and Power Safety in Data Centers | Haining Wang,** University of Delaware
9:50am - 10:00am	**Towards a DDoS Resilient Emergency Dispatch Center | Weidong (Larry) Shi,** University of Houston
10:00am - 10:05am	**INTERNET MEASUREMENT & ATTACK MODELING (IMAM) | PM Introduction: Ann Cox**
10:05am - 10:25am	**From Local to Global Awareness: A Distributed Incident Management System | David Dittrich,** University of Washington, Tacoma
10:25am - 10:35am	MORNING BREAK
10:35am - 10:55am	**Stucco: Collecting and Organizing Security Data for Contextual Understanding | John Goodall,** Oak Ridge National Laboratory
10:55am - 11:15am	**Clique: Understanding Network Traffic Patterns and Behaviors | Dan Best,** Pacific Northwest National Laboratory
11:15am - 11:35am	**Internet Topology and Performance Analytics for Mapping Critical Network Infrastructure** **KC Claffy,** University of California, San Diego
11:35am - 11:50am	**Retro-Future: Looking Back to Look Forward in 2016 | John Heidemann,** University of Southern California Information Sciences Institute
11:50am - 12:05pm	**Attack Modeling: A Case Study of Airspace Vulnerability | Sandip Roy,** Brigham Young University
12:05pm - 12:20pm	**APT Detection via Machine-Based Analysis of Passive DNS | Dave Dagon,** Georgia Tech
12:20pm - 1:20pm	**LUNCH (on own)**

Track 2 continued

○ EARLY ◉ MID ● MATURE

1:20pm - 1:35pm	**Defending Every Thing with Symbiote and FRAK | Ang Cui,** Red Balloon Security
1:35pm - 1:50pm	**Autonomous Detection and Healing of Silent Vulnerabilities | Jeff Gummeson,** BlueRISC
1:50pm - 2:00pm	**Vulnerable Supply Chain Organizations: Identify/Notify | April Lorenzen,** Dissectcyber
2:00pm - 2:10pm	**Robustness in U.S. Equity Markets | Scott Condie,** Brigham Young University
2:10pm - 2:20pm	**Automatic Detection and Patching using Power Fingerprinting in Embedded Systems** Carlos Aguayo Gonzales, Power Fingerprinting
2:20pm - 2:25pm	**CYBER SECURITY COMPETITIONS |** PM Introduction: Edward Rhyne
2:25pm - 2:45pm	**Capitalizing on Competitions for Cybersecurity Career Development | Karen Evans,** Center for Internet Security
2:45pm - 3:05pm	**Comic Based Education and Evaluation for Cyber Security | Laurin Buchanan,** Secure Decisions
3:05pm - 3:15pm	AFTERNOON BREAK
3:15pm - 3:35pm	**The National Collegiate Cyber Defense Competetion (NCCDC) | Dwayne Williams,** University of Texas at San Antonio
3:35pm - 3:40pm	**SOFTWARE ASSURANCE MARKETPLACE (SWAMP) |** PM Introduction: Kevin Greene
3:40pm - 4:00pm	**SWAMP: Advancing Software Assurance through a Continuous Assurance Platform | Miron Livny,** Morgridge Institute
4:00pm - 4:10pm	AFTERNOON BREAK

	GENERAL SESSION
4:10pm - 4:30pm	**Cyber Security Division Performer Awards | Douglas Maughan, DHS S&T CSD Division Director**
4:30pm - 4:35pm	**Conference Wrap-up**

“A distinguishing feature of the Cyber Security Division is their emphasis on tech transfer. CSD wants to make sure the technologies and techniques we are developing actually end up in the hands of the end-user.”

Chris Oehman
Researcher for Pacific Northwest National Laboratory

PANEL SPEAKERS

R&D IN OPERATIONAL ENVIRONMENTS PANEL

The R&D in operational environments panel will include both government and state operators discussing what it takes to support the successful transition of R&D into operational use.

Ann Barron DiCamillo

Director, United States Computer Emergency Readiness Team (US-CERT), Department of Homeland Security, Office of Cybersecurity and Communications

James Darnell

Special Agent in Charge (ATSAIC), United States Secret Service (USSS)

Michael Hamilton

Lead Security Consultant, Critical Informatics; Robert Kaminski, Senior Electronics Engineer, Information Directorate, Air Force Research Laboratory

Robert Kaminski

Senior Electronics Engineer, Information Directorate, Air Force Research Laboratory

Moderator: Scott Tousley, DHS S&T CSD Deputy Director

TECHNOLOGY TRANSITION SUCCESS PANEL

The technology transition success panel will include both developers and investors sharing best practices necessary to successfully transition innovative cybersecurity R&D technologies, tools, and techniques into the marketplace.

Jake Braun

Cambridge Global

Stan Brown

Partner, Ernst & Young LLP

Nicolas M. Chaillan

Founder and Chief Information Security Officer, Cyber Revolution, Inc.

Andrew Hoog

CEO and Co-founder, NowSecure

Joshua Neil

Senior Manager, Security Analytics

Salvatore Stolfo

Director, Red Balloon Security, Inc.

Moderator: Mike Pozmantier, DHS S&T CSD

“The Cyber Security Division is very focused on international partnerships. They actively share their research and results with us. Our relationship is very results focused, making a better cyberspace.”

Eelco Stofbergen
Expertise and Advisory Manager
Dutch National Cyber Security Center, Netherlands

R&D SHOWCASE
FEATURED PRESENTERS

Situ: Discovering Suspicious Behavior in Cyber Security

Presenter: John Goodall, Oak Ridge National Laboratory

Signature-based security systems are effective at detecting known attacks, but are unable to detect novel or sophisticated attacks. Indeed, automated security systems will never be capable of detecting all malicious activity. Network operators need tools to help identify suspicious behavior that bypasses automated security systems.

Situ combines anomaly detection and data visualization to provide a distributed, streaming platform for discovery and explanation of suspicious behavior to enhance situation awareness. This novel approach to anomaly detection is based on unsupervised, probabilistic modeling. Key to the approach is modeling events in different contexts or at multiple scales; each event is modeled and scored by multiple anomaly detectors to identify different kinds of anomalous behavior. The architecture of Situ is designed to scale to very high data rates on commodity hardware—hundreds of thousands of events per second.

A Watchdog System for Internet Routing

Presenter: Christos Papadopoulos, Colorado State University

Leveraging both the software BGPmon and Cyclops, developed under past DHS S&T CSD funding, and the on-going data collection at RouteViews, Colorado State University developed Watchdog System for Internet Routing (WIT), a BGP monitoring system for Australian critical infrastructure. The performer identified critical services and monitored these critical services from locations around the world to provide real-time alerts for new events. Colorado State University also provided long term historical records for tracking behavior under past events.

The system is flexible and can be deployed as a private instance or as part of the public system the performer operates. WIT is scalable and robust through the use of a high-performance distributed database, is lightweight through the use of custom BGP monitoring software, is extensible by accommodating a broad set of monitored data, and enables several types of alerts such as prefix hijacks and routing path anomalies.

R&D SHOWCASE
FEATURED PRESENTERS

Towards a Global Network Reputation System: A Mechanism Design Approach

Presenter: Mingyan Liu, University of Michigan

Networks are under constant security threats from various sources, including botnets, worms, spam, phishing and denial of service attacks. The state of the art in cybersecurity typically focuses on information collected at the individual host and IP address levels, e.g., which IP address has been seen sending out spam collected and distributed by host reputation systems or blacklists (RBLs). While useful in filtering, the highly dynamic nature of IP addresses can severely limit the timeliness and accuracy of these lists. By contrast, information collected on individual hosts or IP addresses can be aggregated in such a way to reveal stable and predictive behavior over time, enabling a more proactive policy design. The project's goal is to build a global network reputation system aimed at providing the data and technology for accurate and quantitative assessment of the security posture at an organizational level.

Federated Command and Control for Adaptive Computer Network Security

Presenter: Marco Carvalho, Florida Institute of Technology

The Federated Command and Control (FC2) effort proposes the research, design and implementation of a resilient framework that enables the federation of cyber operation command and control infrastructures. The goal of the effort is to facilitate the on-demand negotiation of data, policy, and control information sharing across disparate C2 infrastructures, enabling and increasing the overall security of the federated system beyond the levels achievable by the federation members independently. FC2 proposes a distributed, semi-automated and extensible framework using software agents to support both the establishment and maintenance of overlapping federations. Software agents utilize a set of federation infrastructure services to semantically represent, distribute and protect federation member information, and to coordinate responses. The federation infrastructure ensures that data usage and privacy policies implemented by a federation member are enforced and respected by all members. In this presentation Florida Institute of Technology will describe our progress in the FC2 effort, starting from the proposed requirements and design choices, following with the description of the current prototype and initial deployment tests.

R&D SHOWCASE
FEATURED PRESENTERS

Accelerating the Discover, Identification, and Remediation of Application Vulnerabilities with Hybrid Analysis Mapping

Presenter: Dan Cornell, Denim Group

As software systems grow more capable and complex, they become more susceptible to flaws that prospective adversaries can exploit. Application security testing tools – both static (SAST) and dynamic (DAST) - can each provide valuable insight into the security state of software systems, but no one tool provides complete coverage. Denim Group's Hybrid Analysis Mapping (HAM) framework accelerates the discovery, identification, and remediation of application vulnerabilities to help further protect software systems from sophisticated cyber-attacks by correlating the results of multiple SAST and DAST tools. In addition to vulnerability report correlation, the HAM technology helps improve the quality of DAST scanning by pre-seeding scanners with application attack surface information and increases the speed of vulnerability remediation by mapping DAST scan results to specific lines of code in developer IDEs. HAM technology is currently available in Denim Group's ThreadFix software assurance program management platform.

MobileRoT: A Fully Software-based Mobile Security Architecture

Presenter: Kristopher Carver, BlueRISC

BlueRISC's MobileRoT (Mobile Roots-of-Trust) solution is a fully software-based mobile security architecture, spanning both boot-time/static and runtime/dynamic RoTs, mimicking the protection achievable through the use of a dedicated security-centric hardware. The solution supports the industry accepted Trusted Computing Group's (TCG) Mobile Trusted Module (MTM) specification but goes much beyond MTM by providing dynamic trust verification, enabling an open, useable application programming interface (API) to the underlying trusted services, and by supporting government use cases. MobileRoT is a lean solution and requires no manufacturer/service provider support for insertion, while being functionally generic to the platform upon which it is deployed. MobileRoT is established without requiring any modifications to the underlying OS/kernel greatly reducing integration related hurdles to adoption and comes with a fully automated installation procedure. The solution supports multiple usage models ranging from providing protections and controls for off-the-shelf applications to direct utilization of MobileRoT's trusted services within a custom application design via the utilization of MobileRoT's API. To date, MobileRoT has been demonstrated and delivered to strategic partners and early adopters not only for test and utilization but also for custom, protected application development.

R&D SHOWCASE
FEATURED PRESENTERS

Project iVe: Forensics for Vehicle Infotainment and Navigation Systems

Presenter: Ben LeMere, Berla Corporation

Vehicle infotainment and telematics systems store a vast amount of data such as recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been. Many systems may also record events such as when and where a vehicle lights are turned on, which doors are opened and closed at specific locations, and even where the vehicle is located when Bluetooth devices connect. When a vehicle is used in criminal activity it can include valuable digital evidence key to a law enforcement investigation, just like a computer or cell phone. Through DHS S&T CSD funding, Berla is developing the iVe vehicle forensics tool for Federal, State and local law enforcement which inclues a testing user group made up of 17 law enforcement agencies with S&T-provided licenses. iVe is commercially available and currently supports forensic data extraction from over 4,000 different vehicle models.

Protecting Emergency Services from Complex Distributed Telephone Denial of Service

Presenter: Mark Collier, SecureLogix

Telephony Denial of Service (TDoS) is a flood of malicious inbound calls. TDoS has and can target public safety numbers, such as 911 and emergency responders. If coordinated with a physical terrorist attack, the TDoS attack would be particularly disruptive, resulting in a large number of victims not getting through to emergency services. TDoS can also affect financial services, by denying consumers access to voice contact centers. If synchronized with a Distributed Denial of Service (DDoS) attack against a financial service Internet and mobile presence, a TDoS attack can prevent customers from reaching their banks at all. In addition, TDoS is a growing threat because enterprises are migrating to centralized SIP trunking, which creates a centralized choke point.

SecureLogix is working with DHS S&T CSD to develop TDoS defenses for enterprises. The defense uses a series of filters to differentiate legitimate from TDoS calls and quickly treat the malicious calls. The key need is the ability to authenticate callers and detect fraudulent spoofing of information such as the calling number. SecureLogix is focused on solving this issue and also applying it to other voice threats. SecureLogix has completed a Phase i SBIR and is working with the University of Houston on TDoS issues within Next-Generation 911 (NG-911) systems.

R&D SHOWCASE
FEATURED PRESENTERS

DHS IMPACT: Datasets for Use in Cybersecurity Research

Presenter: Paul Royal, Georgia Tech Information Security Center

Leveraging over a decade of experience in large-scale, transparent malware analysis, the Georgia Tech Information Security Center (GTISC) puts information about the network activity of malicious software in the hands of researchers and practitioners to whom this data would otherwise be inaccessible. Through DHS IMPACT (formerly PREDICT), over 150 entities receive daily GTISC malware analysis datasets for use in both research and network defense. These include top-tier academic research centers, government agencies, internet service providers, major financials and various other Fortune 100 companies.

Linking the Oil and Gas Industry to Improve Cybersecurity: Collaborative Research Within the Oil and Natural Gas Industry

Presenter: Barry Cott, Shell

The Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) is an ongoing collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate. LOGIIC undertakes collaborative research and development projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector. The objective is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality. LOGIIC has been active for over 10 years now and has delivered nine research projects over that time, with two more projects currently in execution.

“A lot of today’s solutions weren’t built by single institutions. The Cyber Security Division pulls together different approaches to develop a creative and effective solution to secure our nation.”

Shari Lawrence-Pfleeger
Researcher and 2014 R&D Showcase Presenter

TECHNOLOGY
TOPIC DESCRIPTIONS

CYBERSECURITY RESEARCH INFRASTRUCTURE

Experimental Research Testbed (DETER)

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

DETER Project Website

Research Data Marketplace

The Research Data Marketplace, also known as the Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) program supports the global cyber risk research community by coordinating and developing real world data and information sharing capabilities including tools, models, and methodologies. In order to accelerate solutions around cyber risk issues and infrastructure support, the IMPACT program coordinates data and information sharing between the government, critical infrastructure providers, and the cybersecurity research and development community.

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.

Data Privacy

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

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 Distributed Denial of Service Defense project aims to slow the 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 be given the ability to withstand one tera-bits per second attacks, pushing the defender into the lead.

TECHNOLOGY
TOPIC DESCRIPTIONS

Enterprise Level Security Metrics
Developing meaningful cybersecurity metrics has been challenging, particularly as IT and cyberattack methods have continued to change and evolve, making it difficult for organizations to effectively evaluate their cybersecurity defenses. The Enterprise Level Security Metrics project addresses this by developing practical and useful decision aids and techniques to allow organizations to better gauge and measure their security posture and help users make informed decisions based on threats and cost.

Insider Threat
Cybersecurity defenses are frequently focused on threats from outside an organization, rather than threats posed by untrustworthy individuals inside an organization even though insider threats 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.

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.

Moving Target Defense
Our IT systems are built to operate in a relatively static configuration on hardware that is presumed to be safe and trusted. However, static systems present a substantial advantage to attackers providing them the opportunity to observe the operation of key IT systems over a period of time. The Moving Target Defense (MTD) project is seeking to develop game-changing capabilities that continually modify attack surfaces, making it more difficult for attackers to exploit and attack, and technologies that enable systems to continue to function and meet mission needs while an attack is occurring.

Security of Cloud Based Systems
Cloud computing has changed the way organizations deploy and manage information technology (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 to help mitigate the security implications of cloud computing.

Network Mapping and Measurement
The constantly changing nature of the Internet necessitates that we understand the Internet's foundational elements to improve the user's experience, reduce the cost of measuring the Internet, and protect the nation's cyber infrastructure. The IMAM - Network Mapping and Measurement project provides data about the current state of the Internet, how outages affect user communities, and what can be done to improve network reliability.

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 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 happening, and during the post-attack period.

Resilient Systems and Networks

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

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 spoofing and other attacks in which cyber criminals can redirect users to unsafe websites or pathways. The Secure Protocols for the Routing Infrastructure (SPRI) project's goal is to add security to the internet's core routing protocol, namely Border Gateway Protocol (BGP), so that communication follows the intended path between organizations.

Download Open Source suite for RPKI
Download Open Source Relying Party software

HUMAN-CENTRIC CYBERSECURITY

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.

Cybersecurity Competitions

Ensuring that our nation has a highly skilled cybersecurity workforce is important to maintaining our nation's systems and networks and combating future cyberattacks. The Cybersecurity Competitions project aims to overcome the shortage of cybersecurity professionals by exposing high school and college students to robust and engaging cyber competition challenges. These competition environments also serve as opportunities to expose the students to cutting-edge cyber defense tools and technologies developed within CSD.

National Collegiate Cyber Defense Competition Website | U.S. Cyber Challenge Website

TECHNOLOGY
TOPIC DESCRIPTIONS

Cyber Economic Incentives

Despite the growing focus on cybersecurity there has been little attention from the research community on economic, behavioral and business factors that induce a private organization to select and implement cybersecurity measures. The Cyber Economic Incentives project examines where, why, and how much cyberinfrastructure owners and operators should invest in cybersecurity. This project looks at adoption incentives, commercial network operator's reputations for preventing attacks and understanding criminal behaviors to mitigate risks.

Usable Cybersecurity

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

LAW ENFORCEMENT SUPPORT

Cybersecurity Forensics

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

Anonymous Networks and Currencies

Criminals are increasingly exploiting the privacy-enhancing protections built in for the legitimate use of anonymous networks and cryptocurrencies. Criminal investigations into anonymous networks and cryptocurrencies are resource intensive and challenging; requiring the investment of significant man-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.

SOFTWARE ASSURANCE

Application Security Threat and Attack Modeling (ASTAM)

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 and Threat Attack Modeling (ASTAM) project is designed to bring together contexts from application security testing tools, automate application security testing, and provide continuous monitoring capabilities to keep a monitor application security controls. The goal of the ASTAM project is to create a Unified Threat Management (UTM) system that allows cybersecurity professionals to monitor and to

analyze software systems and applications to identify potential risks like security threats, and exposures to the system environment. The system will then develop 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 us all vulnerable to cyber attacks. The complexity and size in today's software makes it difficult for software quality assurance tools to identify potential weaknesses that expose vulnerabilities in software. The Software Quality Assurance project is designed 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.

Software Assurance Marketplace

Software has become an essential component of our 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 around software security. 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. The SWAMP helps to formalize software assurance in organizations, and provide 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.

SWAMP Website

Static Tool Analysis Modernization Project (STAMP)

The Static Tool Analysis Modernization (STAMP) project is a revolutionary approach to modernize and advance the capabilities found in static analysis tools. The goal of STAMP is to improve tool coverage and to be seamlessly integrated into the continuous software delivery pipelines to achieve "security at-speed" in the software development process. STAMP is focused on closing the gaps in two key areas: research and development, and implementation of new techniques for static software analysis; as well as applying new and improved testing and evaluation capabilities to continuously evolve static analysis to keep pace with modern software.

TRANSITION AND OUTREACH

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 was established and is increasing awareness of open security methods, models, and technologies that provide sustainable approaches to support national cybersecurity objectives.

TECHNOLOGY DEMONSTRATION

Transition to Practice

Transitioning new technologies out of the research laboratory and into the commercial marketplace can be a difficult task. As a top White House priority the Transition to Practice (TTP) project was created to accelerate the transition of cybersecurity research into widespread deployment. The TTP project identifies technologies developed with federal funding at national 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 project accomplishes its mission by developing partnerships and serving as a connection point between the federal research community, network operators, and private industry.

TRUSTWORTHY CYBER 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, enabling secure and resilient service provisioning.

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 organizations, which conducts research to address homeland security challenges. Infrastructures are increasingly 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.

CIRI Website | Homeland Security University Programs Website

Cyber Physical Systems Security

Cyber Physical Systems are defined as smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world. 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 can be 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.

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 cyber-attacks, 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 CREDC consortium will develop solutions through research and development, education, and intense industry engagement. The CREDC model will generate research, evaluate the results and then deploy solutions into the marketplace. The project focus will 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 identify the impact of disruptive technologies, such as the Internet of Things and cloud computing, on EDS resiliency.

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 against it could be disruptive to the nation's daily economic activities. To help secure this sector from cyber-attacks, CSD developed the Distributed Environment for Critical Infrastructure Decision Making Exercises (DECIDE) project – a national cyber war-gaming capability. This capability has resulted in the delivery of simulation-supported cyber exercises to the desktops of critical infrastructure owners and operators – enabling them to create and run exercises that are relevant to their own business interests.

Linking the Oil and Gas Industry to Improve Cybersecurity

In order to address cybersecurity threats to our nation's critical oil and gas infrastructure and their supervisory control and data acquisition systems, CSD led the creation of the public-private consortium Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC). LOGIIC is an ongoing collaboration between DHS, the Automation Federation and five major oil and gas companies. The consortium undertakes collaborative R&D projects to improve the level of cybersecurity in oil and gas critical systems. The objective of LOGIIC is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality.

LOGIIC Website

COLLABORATION SESSIONS

Collaboration Sessions will be held February 18 from 4:15pm - 5:30pm.

TOPIC 1

"Going Dark": Technical Challenges and Potential Solutions

The increasing trend towards encryption (and non-retention of "root keys") by vendors and service providers has created a significant challenge to the DHS critical mission of ensuring national security and public safety. The objective of this session is to share ideas on potential technical and non-technical solutions to meet this challenge, while also safeguarding privacy, promoting free expression, and strengthening cybersecurity.

Moderators: Simson Garfinkel, Chris Soghoian

TOPIC 2

Cyber Security Transition and Commercialization Pathways

Transitioning research projects into widespread operational deployment and use is the end goal of most applied research. There are several pathways to achieve this, including but not limited to: open sourcing, licensing, commercial spin-offs and acquisitions, leading to Federal, State or local government. The objective of this session is to share and discuss the various avenues, techniques and best practices that principal investigators and program managers use to transition their technologies into practice.

Moderators: Mike Pozmantier, Dave Balenson, Bill Arbaugh

TOPIC 3

Measuring Cyber Security R&D Impact

According to Gartner, the IT research and advisory firm, global IT security spending was expected to exceed $71.1 billion in 2014 and $76.9 billion in 2015. Measuring the impacts of this increased investment, however, has proven to be a difficult challenge. For example, does a decreased dwell time mean detection schemes are improving, or are the intrusions merely becoming harder to detect? The objective of this session is to share ideas on how to measure the impact that R&D contributes to the overall cyber security posture and enable DHS S&T to more effectively measure and report the value added from its R&D investments.

Moderator: Zach Tudor

TOPIC 4

"Blue Sky" Session

A Blue Sky discussion is intended to collect creative ideas that are not limited by current thinking or beliefs. The scale and complexity of the cyber security challenge lends itself to an unconstrained "art of the possible" discussion that would enable cyber security defenders to leapfrog the current attacker advantage. For example, what cyber security challenges will we face in 3, 5, or 10 years? What ideas are needed to address those challenges that are radically different from our current thinking?

Moderators: Marcus Sachs, Ulf Lindqvist

TOPIC 5

Cyber Economic Incentives and Insurance

A continuing challenge involves incentivizing critical infrastructure providers and commercial companies to invest more in cyber security to protect critical data and assets. Research into this less traditional area of cyber security has grown as the community recognizes the need for a multi-disciplinary approach. Economic analysis of incentives, including cyber insurance, helps explain why individuals and organizations do (or do not) take action to detect and mitigate cybersecurity threats. The objective of this session is to discuss cyber insurance and potential research topics to better understand the space, including the potential ethical concerns associated with insurance programs.

Moderators: Tom Finan, Tony Cheesebrough

“I think LOGIIC is a great opportunity for Chevron. This consortium allows us to truly partner with the government to address cybersecurity industrial control systems together.”

Penny Wolter
PCN Security Program Manager for Chevron and LOGIIC member

PERFORMER AWARDS

We are proud to announce the first annual DHS S&T CSD R&D Showcase and Technical Workshop Meeting Awards. Safeguarding and Securing Cyberspace and building a Trusted Cyber Future are central pillars of the DHS S&T mission. CSD funded researchers work is integral to improving federal cybersecurity R&D and the awards below highlight their outstanding efforts in the CSD portfolio.

"BANG FOR THE BUCK" AWARD

Awarded to an effort with a large impact for a relatively small budget

"CYBER IS A GLOBAL SPORT" AWARD

Awarded to an effort that has an international involvement and impact

"CROSSING THE VALLEY OF DEATH" AWARD

Awarded to an effort that has a technical transition success story

"BUILDING TOMORROW'S WORKFORCE" AWARD

Awarded to an effort that is helping to develop the next generation of cybersecurity professionals

"SIGNIFICANT GOVERNMENT IMPACT" AWARD

Awarded to an effort which has had a significant impact on government

CONNECT WITH US

ONLINE AT:
DHS S&T Cyber Security Division Website

EMAIL
DHS S&T Cyber Security Division email address

TWITTER
DHS S&T Cyber Security Division Twitter page

FACEBOOK
DHS S&T Cyber Security Division Facebook page

YOUTUBE
DHS S&T Cyber Security Division YouTube page

FRONT OFFICE	EMAIL ADDRESS
Douglas Maughan	Email Douglas Maughan
Scott Tousley	Email Scott Tousley
Melissa Ho	Email Melissa Ho
Robert Knetl	Email Robert Knetl

PROGRAM MANAGER	PROGRAMS	EMAIL
Ann Cox	Internet Measurement and Attack Modeling (IMAM)	Email Ann Cox
Chase Garwood	Cyber Physical Systems Security (CPSSEC)	Email Chase Garwood
Kevin Greene	Software Assurance Marketplace (SWAMP), Software Quality Assurance, Static Tool Analysis Modernization Project (STAMP) and Application Security Threat and Attack Modeling (ASTAM)	Email Kevin Greene
Eric Harder	Next Generation Cyber Infrastructure - Apex	Email Eric Harder
Robert Hickey	Aircraft Cyber Evaluation (ACE)	Email Robert Hickey
Anil John	Data Privacy and Identity Management	Email Anil John
Erin Kenneally	Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT), formally known as Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT)	Email Erin Kenneally
Joseph Kielman	Cyber Economic Incentives	Email Joseph Kielman
Megan Mahle	Anonymous Networks and Currencies, Cybersecurity Forensics, Insider Threat, and Mobile Wireless Investigations	Email Megan Mahle
Daniel Massey	Cyber Physical Systems Security (CPSSEC), Distributed Denial of Service Defense (DDoSD), Homeland Open Security Technologies (HOST), and Secure Protocols for the Routing Infrastructure (SPRI)	Email Daniel Massey
Michael Pozmantier	Transition to Practice (TTP)	Email Michael Pozmantier
Edward Rhyne	Cybersecurity Competitions, Moving Target Defense (MTD), and Secure Cloud Computing	Email Edward Rhyne
Gregory Shannon	Detailed to OSTP as the Assistant Director for Cybersecurity Strategy	Email Gregory E. Shannon
Vincent Sritapan	Mobile Device Security	Email Vincent Sritapan
Erin Walsh	Critical Infrastructure Design and Adaptive Resilient Systems (CIDARS)	Email Erin Walsh
Gregory Wigton	Cybersecurity for O&G Systems (COGS), Cybersecurity for Energy Systems (CES), Enterprise Level Security Metrics and Usable Cyber Security, and Next Generation Cyber Infrastructure - APEX	Email Gregory Wigton

CYBER SECURITY DIVISION TEAM

FRONT OFFICE

Douglas Maughan
Director

Scott Tousley
Deputy Director

Melissa Ho
Managing Director SVO

Robert Knetl
Senior Advisor

Michael Costello
Finance Support

Ann Dutton
Communications Support

Brendon Gibson
Technical and Program Support

Melissa Mann
International Partnerships

Jennifer Mekis
Finance Support

Shelby Smith
Communications Support

Lauren Tarnoski
Business Operations Support

PROGRAM MANAGERS

Ann Cox
Program Manager

Chase Garwood
Program Manager

Kevin Greene
Program Manager

Eric Harder
Program Manager

Robert Hickey
Program Manager

Anil John
Program Manager

Erin Kenneally
Program Manager

Joseph Kielman
Program Manager

Megan Mahle
Program Manager

Daniel Massey
Program Manager

Michael Pozmantier
Program Manager

Edward Rhyne
Program Manager

Gregory Shannon
Detailed to OSTP as the Assistant Director for Cybersecurity Strategy

Vincent Sritapan
Program Manager

Gregory Wigton
Program Manager

Not pictured: Erin Walsh, Program Manager

CYBER SECURITY DIVISION TEAM

SUPPORT STAFF

Mario Ayala
Program Support

Matt Billone
Program Support

Amelia Brown
Program Support

John Drake
Program Support & International Partnership Coordination

Jeffrey Dewhurst
Program Support

Tammi Fisher
Program Support

Russell Madison
Program Support

Burak Pehlivan
Program Support

Noemi Rodriguez
Program Support

Yolanda Saunders
Program Support

Ike Smith
Program Support

Ryan Triplett
Program Support

Not pictured: Jennifer Peters, Program Support

“S&T has supported our project in keeping us connected and assisting us with opening doors to help transition our product into the marketplace.”

Mike Hamilton
Former CSD Principal Investigator of the PRISEM project

UPCOMING EVENTS

RSA Conference 2016

February 29 - March 3, 2016 | Moscone Center | San Francisco, California

South Expo Hall – Booth 2633

Engage with the DHS S&T CSD at the RSA Conference Expo. This year, CSD will feature government funded R&D technologies, tools and techniques to address today's challenging cybersecurity landscape.

Connect with us on Twitter by following #RSAC and #CyberResearch
Register with comp code XEDHSTCH16 at: RSA 2016 registration Website

EXPO HOURS:	
Monday, February 29	5:00pm – 7:00pm (Welcome Reception)
Tuesday, March 1	10:00am – 6:00pm
Wednesday, March 2	10:00am – 6:00pm (Pub Crawl from 5:00 PM - 6:00 PM)
Thursday, March 3	10:00am – 3:00pm

2016 Government Cyber Security SBIR Workshop

Summer 2016 | Washington, DC

The 2016 Government Cyber Security Small Business Innovation Research (SBIR) Workshop will focus on maximizing technology transition opportunities for SBIR funded research. The workshop will feature short presentations by funded small businesses describing their products and technologies, prime contractors identifying their programs and needs and government stakeholders describing their mission and requirements. Private one-on-one sessions will be held for integrators, government, and/or investors to discuss partnering, tech transition and business opportunities with small businesses.

For more information follow dhsscitech Twitter page, #CyberSBIR on Twitter or email the 2016 Government Cyber Security SBIR Workshop.
Registration is complimentary.

TRANSITION TO PRACTICE EVENTS

The Transition to Practice (TTP) program, part of the White House's Federal Cybersecurity R&D Strategic Plan and Comprehensive National Cybersecurity Initiative (CNCI); works to identify emerging cybersecurity technologies that were developed with Federal funding and help them transition into products capable of broad utilization. The program also provides a connection point for cybersecurity researchers, the federal government and the private sector to transition technology from research labs to the HSE and the commercial marketplace.

Registration for all technology demonstration events are complimentary for public and private sector cybersecurity practitioners, technology investors, system integrators and information technology companies

For more information email TTP and follow dhsscitech Twitter page and #TTPDemo on Twitter.

FY15 Transition to Practice Technology Demonstration Days

The FY15 TTP technology class features seven innovative cybersecurity technologies developed at the Department of Energy (DOE) and Department of Defense (DOD) Laboratories. During these technology demonstrations, cybersecurity professionals from various sectors including the Federal Government and Oil & Gas Sector will learn about these new technologies through presentations, demonstrations, and discussions with the research teams that produced these technologies. In addition, attendees may discuss opportunities for piloting the technologies and areas of interest to drive further cybersecurity research.

Government | Spring 2016 | Washington, DC

Energy Sector | Spring 2016 | Houston, Texas

FY16 Transition to Practice Technology Demonstration Days

The FY16 TTP technology class features eight innovative cybersecurity technologies developed at the DOE and DOD Laboratories. During these technology demonstrations, cybersecurity professionals from various industries including the Federal Government, Private Sector, and Finance Sector will learn about these new technologies through presentations, demonstrations, and discussions with the research teams that produced these technologies. In addition, attendees may discuss opportunities for piloting the technologies and areas of interest to drive further cybersecurity research.

Government | Spring 2016 | Washington, DC

Investors, Integrators, and IT Companies (I3) West | Summer 2016 | Silicon Valley, California

Investors, Integrators, and IT Companies (I3) East | Summer 2016 | Washington, DC

Finance Sector | June 2016 | New York City, New York

LOGISTICS

R&D SHOWCASE | FEBRUARY 17

Registration

Registration will begin at 7:15AM
Location: Palm Court Ballroom

General Session

The General Session will begin at 8:15AM
Location: Grand Ballroom

The R&D Showcase featuring nine innovative solutions and two collaborative projects with the private sector that address a variety of complex cybersecurity challenges.

Technology Demonstration/Poster Session

Beginning at 3:30pm, in the East and State Room, the Technology Demonstration and Poster session will feature the division's entire portfolio.

R&D TECHNICAL WORKSHOP | February 18-19

Registration

Registration will begin at 7:30AM
Location: Promenade Foyer in front of the Grand Ballroom

General Session

The General Session will begin at 8:30 AM
Location: Grand Ballroom.

Technical Tracks

Daily, in the Grand Ballroom and Palm Court rooms, the technical tracks will feature CSD funded research and technologies.

Collaboration Sessions

Collaboration sessions will be offered to conference participants on Thursday, February 18 from 4:15pm - 5:30pm.

BEVERAGE SERVICE

Water stations will be provided in the registration area and general session.

INTERNET

Participants have been provided with wireless Internet. Please limit access to one personal device.
SSID: Mayflower Conference | Password: CyberShowcase16

SURVEY

Please complete the electronic survey rating your experience at the 2016 R&D Showcase and Technical Workshop. The survey can be found at: **survey Website**

EATERY INFORMATION

1. **Edgar Bar & Kitchen On-Site**
   1127 Connecticut Avenue, NW
   Washington, DC 20036
   Phone: 202-347-2233
2. **Subway**
   1712 L Street, NW
   Washington, DC 20036
   Phone: 202-785-7825
3. **Au Bon Pain**
   1724 L Street. NW
   Washington, DC 20036
   Phone: 202-331-4190
4. **Starbucks**
   1734 L Street, NW
   Washington, DC 20036
   Phone: 202- 293-9180
5. **Kellari Taverna**
   1700 K Street, NW
   Washington, DC 20006
   Phone: 202-535-5274
6. **BLT Steak DC**
   1625 I Street, NW
   Washington, DC 20006
   Phone: 202-689-8999
7. **I Ricchi**
   1220 19th Street, NW
   Washington, DC 20036
   Phone: 202-835-0459
8. **Nando's Peri Peri**
   1210 18th Street, NW
   Washington DC 20001
   Phone: 202-621-8603
9. **Equinox**
   818 Connecticut Ave., NW
   Washington, DC 20006
   Phone: 202-331-8118
10. **Corner Bakery**
    L Street, NW #101
    Washington, DC 20036
    Phone: 202-776-9052
11. **Le Pain Quotidien**
    800 17th Street
    Washington, DC 20006
    Phone: 202-688-0341
12. **Panache**
    1725 DeSales Street, NW
    Washington, DC 20036
    Phone: 202-293-7760
13. **Daily Grill**
    1200 18th Street, NW
    Washington, DC 20036
    Phone: 202-822-5282
14. **Morton's The Steakhouse**
    1050 Connecticut Ave.
    Washington, DC 20036
    Phone: 202-955-5997

NOTES

thank you

for attending the

R&D SHOWCASE & TECHNICAL WORKSHOP

After three busy days – and a packed agenda – we hope you found value in our research projects. We want to hear from you, so let's keep the conversation going. **Stay in touch!**

- DHS Science and Technology website
- DHS Science and Technology email address
- DHS Science and Technology Twitter page
- DHS Science and Technology Facebook page
- DHS Science and Technology YouTube channel

This page intentionally left blank.

Homeland Security

Science and Technology

DHS S&T Cyber Security Division

Securing YOUR Cyber Future