



Defence Research and  
Development Canada

Recherche et développement  
pour la défense Canada

CAN UNCLASSIFIED



DRDC | RDDC  
technologysciencetechnologie

# Department of Homeland Security (DHS) Science and Technology (S&T) programs and cybersecurity showcase

*Lessons learned and recommendations*

Helen Tang  
Ron Burman  
DRDC – Centre for Security Science

**Defence Research and Development Canada**

**Reference Document**

DRDC-RDDC-2018-D045

May 2018

CAN UNCLASSIFIED



## CAN UNCLASSIFIED

### IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Disclaimer: Her Majesty the Queen in right of Canada, as represented by the Minister of National Defence ("Canada"), makes no representations or warranties, express or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

Endorsement statement: This publication has been published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

## **Abstract**

---

This report serves two purposes. The first is to summarize the highlights and lessons learned from the Department of Homeland Security (DHS) Cybersecurity Research and Development (R&D) Showcase and Technical Workshop (Cybersecurity Showcase in short). The second is to inform Defence Research and Development Canada Center for Security Science (DRDC CSS) program formulation by presenting the DHS S&T programs that are relevant to DRDC CSS and explore potential collaboration opportunities that can be leveraged with DHS Science and Technology (S&T).

## **Significance to defence and security**

---

This report informs DRDC CSS program formulation by presenting the DHS S&T programs that are relevant to DRDC CSS and explore potential collaboration opportunities that can be leveraged with DHS S&T.

## Résumé

---

Ce rapport a deux objectifs. Le premier consiste à résumer les faits saillants et les leçons retenues du salon et de l'atelier technique de R et D sur la cybersécurité du DHS (salon cybersécurité en abrégé). Le deuxième est de rendre compte de la composition du programme de RDDC CSS en présentant les programmes de S et T du DHS qui lui sont pertinents et d'explorer les possibilités de collaboration éventuelle grâce à la S et T du DHS.

## Importance pour la défense et la sécurité

---

Dans ce rapport, on rend compte de la composition du programme de RDDC CSS en présentant les programmes de S et T du DHS qui lui sont pertinents et on explore les possibilités de collaboration éventuelle grâce à la S et T du DHS.

# Table of contents

---

Abstract . . . . .	i
Significance to defence and security . . . . .	i
Résumé . . . . .	ii
Importance pour la défense et la sécurité . . . . .	ii
Table of contents . . . . .	iii
List of tables. . . . .	iv
1 Introduction . . . . .	1
2 DHS programs and research areas . . . . .	2
2.1 Silicon Valley Innovation Program (SVIP) . . . . .	2
2.2 International engagement strategy: Bi-Lat Broad Area Announcement (BAA) . . . . .	2
2.3 Centers of Excellence (CoEs). . . . .	2
2.4 Innovation training program . . . . .	2
2.5 Cyber physical systems security . . . . .	3
2.6 Mobile device security . . . . .	3
2.7 Identity management . . . . .	3
3 Recommendations . . . . .	4
References . . . . .	5
Annex A Details of the DHS S&T Programs . . . . .	6
A.1 Silicon Valley Innovation Program (SVIP) . . . . .	6
A.2 International Engagement Strategy: International Broad Area Announcement (BAA) . . . . .	7
A.3 Innovation training program . . . . .	7
A.4 DHS Center of Excellence . . . . .	8
A.5 Cyber physical systems security . . . . .	9
A.6 Mobile device security . . . . .	10
A.7 Identity management . . . . .	10
A.8 Other DHS S&T Divisions and Programs . . . . .	11
Annex B Workshop agenda. . . . .	12

**List of tables**

---

Table B.1: Workshop Agenda. . . . . 12

# 1 Introduction

---

This report serves two purposes. The first is to summarize the highlights and lessons learned from the Department of Homeland Security (DHS) Cybersecurity Research and Development (R&D) Showcase and Technical Workshop (Cybersecurity Showcase in short). The second is to inform Defence Research and Development Canada Center for Security Science (DRDC CSS) program formulation by presenting the DHS S&T programs that are relevant to DRDC CSS and explore potential collaboration opportunities that can be leveraged with DHS S&T.

The DHS annual Cyber Security Division (CSD) R&D Showcase and Technical Workshop is the US federal government's largest cybersecurity R&D conference. It is a special platform where the DHS S&T Cyber Security Division (CSD) introduces its funded research projects. There are 115 technology presentations featuring \$250 million of CSD-funded R&D projects that cover cyber physical systems security, mobile security, cybersecurity research infrastructure, support for law enforcement, identity management, data privacy and 10 more research topics. The Cybersecurity Showcase included presentations of 10 transition-ready projects and 60 technology demonstrations. More than a thousand people attended this event this year held in Washington DC, July 10–13, 2017. DRDC CSS staff members, Dr. Helen Tang and Mr. Ron Burman, attended the Cybersecurity Showcase. Afterwards, Helen performed further investigations and follow-up work to broaden the knowledge of DHS S&T programs and explore potential collaboration opportunities with DHS S&T.

The Cybersecurity Showcase provided exposure to a wide variety of programs and many research areas of DHS S&T. Below we briefly introduce seven programs that are most relevant to DRDC CSS. More details can be found in Annex A and B.

## **2 DHS programs and research areas**

---

### **2.1 Silicon Valley Innovation Program (SVIP)**

Launched in 2015, SVIP engages and funds technology startups to help develop solutions for DHS components and other Homeland Security Enterprise entities. SVIP has issued solicitation calls for the following topics: Internet of Things security; enhancements to the Global Travel Assessments System; Airport Passenger Processing; small, unmanned aircraft system capabilities; K-9 wearables; and cybersecurity for the financial services sector. We can collaborate with the SVIP program to access the newest technology at Silicon Valley. One program manager had agreed to share some of the results and documentation of RF Network security technology with CSS.

### **2.2 International engagement strategy: Bi-Lat Broad Area Announcement (BAA)**

DHS S&T presented its international engagement strategy which includes the new International BAA initiative announced February 2017 (\$9.5M in five years). The first Bi-lat BAA is between the US and the Netherlands. International partners were invited to present their own government funded innovations at the Cyber Showcase. Specifically, Israel, New Zealand, UK, Singapore and the Netherlands had their representatives present at the workshop.

There were a few Canadian companies that presented at the showcase (they work directly with DHS): Securekey, Kdmtechnologies and ICS Secure. CSS has co-funded a couple of projects with DHS in Cyber R&D and could collaborate more in the future and present next year.

### **2.3 Centers of Excellence (CoEs)**

The DHS S&T Centers of Excellence (CoEs) develop multidisciplinary, customer-driven, homeland security science and technology solutions and help train the next generation of homeland security experts.

Currently there are nine CoEs on various security and safety topics. The CoE model and the facility/resources could be beneficial to the Innovation for Defence Excellence and Security (IDEaS) program as well as the Canadian Safety and Security Program (CSSP). One of the CoEs: Critical Infrastructure Resilience Institute (CIRI) is particularly relevant.

### **2.4 Innovation training program**

DHS S&T research program had used SRI International's Innovation Training [1], including the Five Disciplines of Innovation and Value Creation Workshop and the Ideation Workshop which could serve as good references for the IDEaS program and CSSP. SRI is willing to collaborate with CSS and provide a similar training program if we like.

## **2.5 Cyber physical systems security**

DHS has a large Cyber-Physical Systems Security program (CPSSEC). Thirteen projects were presented to address the security issues related to buildings, vehicles, medical devices, smart grid, manufacturing, etc.

DRDC has co-funded two projects related to transportation security and has established a very good collaborative relationship.

## **2.6 Mobile device security**

This program generated a Report to Congress entitled "Study on Mobile Device Security" [2] which could be a good reference for Canada. One project provided a user authentication framework that can allow device and user profiles to be transferred or shared among devices. This addressed one big challenge of the Identity, Credential, Access Management (ICAM) of the Public Safety Broadband Network (PSBN) where a device can be shared among multiple users.

## **2.7 Identity management**

This program helps government program managers with the research and development expertise as well as the required resources to enhance the security and trustworthiness of their programs. The mission of the Identity Management research projects is to develop, test, and evaluate interoperable tools, technologies, standards, and protocols for the purpose of controlling user access within and outside of organizational boundaries. One project "Emergency Responder Authentication System for Mobile Users" could be a good reference for PSBN-ICAM.

### 3 Recommendations

---

This workshop provided great value and highlighted many lessons learned. The following recommendations can be applied to DRDC's CSSP:

- This workshop provided great exposure for the CSSP. Some CSSP led projects receive funding from DHS S&T. By attending the workshop every year, and specifically, volunteering to present the status of R&D projects in Canada through the CSSP and IDEaS program, will create more visibility for CSSP and generate more collaborative funding opportunities from the international community;
- The DHS CSD program has many synergies with the CSSP and IDEaS program. Following up with key contacts from the various DHS S&T projects that have similarities and mutual interest will create collaboration opportunities;
- Every program has a semi-annual review/principal investigator (PI) meeting which is a great opportunity to learn and be exposed to the most recent research. CSS staff (Helen Tang) was invited to participate in the CPSSEC PI meeting and found it to be a very valuable experience to learn the state-of-the-art as well as establish good contact with the program managers and researchers;
- The DHS S&T Centers of Excellence (CoEs) develop multidisciplinary, customer-driven, homeland security science and technology solutions to help train the next generation of homeland security experts. There is an opportunity to leverage these CoEs as they could be beneficial for the IDEaS program and CSSP;
- Emulate the effective engagement strategy that the Innovation Program and SVIP use to access the cutting edge technology from industry and academia;
- Disseminate the knowledge gleaned from this workshop with our partners. After the workshop, Helen Tang briefed Public Safety Canada, Health Canada and Public Health Agency Canada (PHAC) regarding some of the key research projects which was highly appreciated by the partners. Given the travel budget cut, it is important to extract maximize value from this workshop;
- Connect other programs at the DHS S&T listed in Annex A.8) such as Borders & Maritime Security Division (BMD) and Resilient Systems Division (RSD);
- The workshop provided a forum to compare our work being done within CSSP with our international counterparts. The argument could be made that Canada's R&D spending is quite low in comparison and we could benefit from improved collaboration with the private sector.

## References

---

- [1] SRI International Innovation Program overview: <https://www.sri.com/innovation-programs>, accessed on August 1, 2017.
- [2] “Study on Mobile Device Security,” prepared by the Department of Homeland Security (DHS) in consultation with the National Institute of Standards and Technology (NIST), available at: <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>, accessed on August 1, 2017
- [3] Silicon Valley Innovation Program overview: <https://scitech.dhs.gov/hsip>, accessed on August 1, 2017.
- [4] DHS S&T Cyber Security Division Five-Year International Collaboration Broad Agency Announcement (BAA), [https://www.fbo.gov/index?s=opportunity&mode=form&id=2630ac7104fc1764f860079ddee33724&tab=core&\\_cview=1](https://www.fbo.gov/index?s=opportunity&mode=form&id=2630ac7104fc1764f860079ddee33724&tab=core&_cview=1), accessed on September 1, 2017.
- [5] DHS S&T Centers of Excellence (COEs) overview: <https://www.dhs.gov/science-and-technology/centers-excellence>, accessed on September 1, 2017.
- [6] Arctic Domain Awareness Center overview: <http://adac.uaa.alaska.edu>, accessed on September 1, 2017.
- [7] Critical Infrastructure Resilience Institute (CIRI) overview, <https://www.ciri.illinois.edu>, accessed on September 1, 2017.

## Annex A Details of the DHS S&T Programs

---

### A.1 Silicon Valley Innovation Program (SVIP)

The SVIP [3], which launched in late 2015, is the first Homeland Security Innovation Programs (HSIP) regional program. These regional programs will help companies better understand DHS, S&T, DHS components, the homeland security mission, and how these innovation corridors can help the government solve problems across the Homeland Security Enterprise.

The SVIP is expanding DHS'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. DHS is reaching out to Silicon Valley and all of the innovation communities across the nation to harness the commercial R&D ecosystem for government applications, co-invest in ideas and accelerate transition-to-market. Here are three highlights of this program:

- Open to all innovation ecosystems, on-going applications reviewed monthly or quarterly, topic-dependent;
- Three phase funding structure, up to \$800K over 24 months;
- If invited to pitch, decision made the same day, contract awarded under 45 days.

During the conference, the program director provided an overview of this program. Sponsored companies presented their technologies in the following three categories: IoT Security, Drone, Big Data. Below are some companies and their technologies:

- **Bastille**: presented their RF network security product: which is an Enterprise threat detection solution through Software Defined Radio (SDR). It claims to provide full visibility into the known and unknown mobile, wireless and Internet of Things (IoT) devices inside an enterprise's corporate airspace with "RF" frequencies that fall in the 60MHZ to 6GHZ.

**Note:** Helen followed up with the DHS program manager for this company. He agreed to share the results and documents of the trial DHS and NSA had conducted with this company. Helen also followed up with its Canadian representative, Syner Solutions and potential client, Public Safety Canada. The ability to see all emanating devices would provide better situational awareness. This technology could have potential applications for G7, Parliament Hill, etc.

- **Shield AI**: presented an AI technology called Hivemind that ingests data from robotic and software systems to learn and formulate new skills—with Hivemind, robots and analytics software continuously improve and become more capable. They are developing an algorithm that can help Unmanned Aerial System (UAS) travel in unknown terrain, which could be suitable for border surveillance and indoor combat situations.

**Note:** This could be helpful for some DND projects, such as Counter-UAS and Contest Urban Environment (CUE).

- **Factom**: They presented their Blockchain Plugin for Tamper Proof IoT Devices.
- **Ionic**: They presented their IoT security technologies including: device authentication, message confidentiality & integrity, and detailed transaction logging.

- **QED:** It provides a robust, vendor agnostic solution for validating IoT device firmware and software updates.
- **Tamr Inc.** They presented their technology to help big enterprises make sense of disparate data by fusing machine learning with existing knowledge of the data to automate the rapid unification of data silos.

## **A.2 International Engagement Strategy: International Broad Area Announcement (BAA)**

DHS S&T Cyber Security Division Five-Year International Broad Agency Announcement (BAA) [4] released in Feb. 2017 to initiate joint solicitations and targeted research and development. This five-year, \$9.5 million BAA will be used to facilitate cooperative cybersecurity R&D activities with CSD's current and future international partners including Canada.

The first joint call is between US and the Netherlands, which is announced mid-May with \$2.6M to promote the formation of joint U.S.-Dutch research teams. The two research focus areas for the bilateral call are Industrial Control Systems/Supervisory Control and Data Acquisition (SCADA) and Distributed Denial of Service Defenses (DDoS). In all, the partners plan to fund up to five unified research proposals that detail a full program of work to be conducted by teams comprised of academia, industry and laboratory researchers from both countries. Under the program, half of the R&D funding will be provided by CSD through its International Broad Agency Announcement (BAA). Meanwhile, Netherlands Organisation for Scientific Research (NWO) will award funding for the other half of the program to researchers based in the Netherlands.

## **A.3 Innovation training program**

SRI International is an independent non-profit research and development organization. Since 2004, SRI has helped develop DHS S&T's cyber security research and development program, including providing an innovation training program for the program managers.

The innovation program [1] includes: five Disciplines of Innovation and Value Creation Workshops. One of the workshops is particularly interesting: Ideation workshop, which could be quite beneficial to CSS and the IDEaS program. Below is a brief introduction on this workshop:

For an Ideation Workshop, SRI assembles a group of technology and business experts to work side by side with your staff. The workshops are divided into three segments: technology overview, scenario creation and demonstration design. Workshop deliverables includes: technology presentations, use case scenarios, scenario evaluations, selection framework and rankings, demonstration system design, detailed task outlines, and short-term & long-term roadmaps.

The DHS S&T CSD program puts emphasis on applied sciences that meet the customers' needs and transition activities. All the project presentations used the same slide template as a result of the SRI innovation training program. The templates included: customer needs, approach, benefits, competition, transition activities, etc. which could be referenced for some of the CSS project review meetings.

## A.4 DHS Center of Excellence

The DHS S&T Centers of Excellence (CoEs) [5] develop multidisciplinary, customer-driven, homeland security science and technology solutions to help train the next generation of homeland security experts. The CoEs could be beneficial for the IDEaS program and CSSP.

Currently, there are nine CoEs:

- **Arctic Domain Awareness Center of Excellence (ADAC)** [6], led by the University of Alaska Anchorage, develops and transitions technology solutions, innovative products, and educational programs to improve situational awareness and crisis response capabilities related to emerging maritime challenges posed by the dynamic Arctic environment.
- **Borders, Trade, and Immigration Institute (BTI)**, led by the University of Houston, develops technology-based tools, techniques, and educational programs for border management, immigration, trade facilitation, and targeting and enforcement of transnational borders.
- **The Center for Accelerating Operational Efficiency (CAOE)**, led by Arizona State University, applies advanced analytical tools to optimize efficiency in homeland security operations.
- **Center of Excellence for Awareness and Localization of Explosives-Related Threats (ALERT)**, led by Northeastern University, develops new means and methods to protect the nation from explosives-related threats.
- **The Criminal Investigations and Network Analysis Center (CINA)**, led by George Mason University, develops strategies and solutions to enhance criminal network analysis, forensics, and investigative processes for on-the-ground use by agents and officers to predict, thwart, and prosecute crimes.
- **Coastal Resilience Center of Excellence (CRC)**, led by the University of North Carolina at Chapel Hill, conducts research and education to enhance the Nation's ability to safeguard people, infrastructure, and economies from catastrophic coastal natural disasters such as floods and hurricanes.
- **Critical Infrastructure Resilience Institute (CIRI)** [7], led by the University of Illinois at Urbana-Champaign, conducts research and education to enhance the resilience of the Nation's critical infrastructure and its owners and operators.
- **Maritime Security Center of Excellence (MSC)**, led by Stevens Institute of Technology, enhances Maritime Domain Awareness and develops strategies to support Marine Transportation System resilience and educational programs for current and aspiring homeland security practitioners.
- **National Consortium for the Study of Terrorism and Responses to Terrorism (START)**, led by the University of Maryland, provides policy makers and practitioners with empirically grounded findings on the human elements of the terrorist threat and informs decisions on how to disrupt terrorists and terrorist groups.

The CIRI was presented at the conference. CIRI is led by the University of Illinois with an association of sixteen universities, national laboratories, and private companies. It is developing new technologies and business approaches to improve the security and resiliency of critical infrastructure. Private entities own and operate most of the nation's critical infrastructures. The need for more knowledge, resources and

tools to protect these entities from cyber-attacks and complications is essential to the nation's security. The latest round of CIRI funding supports a blend of new projects and ongoing projects that are now entering an advanced phase. The projects are diverse, but they each align under one of four frameworks that drive CIRI's scientific exploration: (1) Insurance and the Business Case for Resilience, (2) Infrastructure Dependencies and Interdependencies, (3) Industrial Supply Chains, and (4) Communication. Researchers will explore topics ranging from securing port infrastructure to creating economic resilience models that help decision makers use cost-effective tactics during pre-disaster planning and post-disaster recovery. Projects funded through CIRI for implementation in early 2017 include the following:

- **Resilience Governance for Infrastructure Dependencies and Interdependencies**—Steve Flynn, Northeastern University.
- **LEFT: An LTE-Oriented Emulation-Instrumented Fuzzing Testbed**—Guanhua Yan, Binghamton University, SUNY.
- **Mapping Infrastructure Interdependencies for Improved Emergency Management and Resilience Investment Decisions**—Iris Tien, Georgia Institute of Technology.
- **Measuring Business and Economic Resilience in Disasters**—Adam Rose, University of Southern California.
- **Community Resilience and Disaster Costs**—Sally Ann McConkey, University of Illinois.
- **Scenario-based Flood Risk Mapping**—Himanshu Grover, University of Washington.
- **Cybersecurity Assurance for Critical Infrastructure**—John Villasenor, UCLA (Stanford University, lead).
- **Identifying and Reducing Barriers to Infrastructure Insurance**—Howard Kunreuther, University of Pennsylvania.
- **Strengthening Local and Regional Regulatory Capacities for Cyber-Resilience**—Rebecca Slayton, Cornell University (Stanford University, lead).
- **Quantifying Interdependencies of the Logical/Physical Internet Topologies**—Kimberly Claffy, University of California, San Diego.
- **Towards Community Resilience through Comprehensive Risk Assessment for Business Continuity**—Jay P. Kesan, University of Illinois.
- **Assessment and Measurement of Port Disruptions**—Gabriel Weaver, University of Illinois.
- **Dynamic Resiliency Modeling and Planning for Interdependent Critical Infrastructures**—Quanyan Zhu, New York University.

## A.5 Cyber physical systems security

The Cyber Physical Systems Security (CPSSEC) program addresses security concerns for Cyber Physical Systems (CPS) and the Internet of Things (IoT). CPS and IoT play an increasingly important role in critical infrastructure, government and everyday life. Automobiles, medical devices, building controls and the smart grid are examples of CPS. Each includes smart networked systems with embedded sensors, processors and actuators that sense and interact with the physical world and support real-time, guaranteed performance in safety-critical applications. The closely related area of IoT continues to emerge and

expand as costs drop and the confluence of sensors, platforms and networks increases. Whether referencing the forward collision prevention capability of a car, a medical device's ability to adapt to circumstances in real-time, or the latest IoT innovation, these systems are a source of competitive advantage in today's innovation economy and provide vast opportunities for DHS and Homeland Security Enterprise missions. However, CPS and IoT also increase cyber security risks and attack surfaces. The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment. Proactive and coordinated efforts are needed to strengthen security and reliance for CPS and IoT.

Thirteen projects were presented in this program track. DRDC had co-funded two transportation cybersecurity projects. The project "Medical Device Risk Assessment Platform" is quite interesting. It addresses the cybersecurity issues in connected medical device, which is an emerging area. Helen briefed Health Canada, Public Health Agency Canada (PHAC) and Public Safety Canada on this project and facilitated potential collaborations between them and the US researchers.

## **A.6 Mobile device security**

Nowadays, the workforce has become increasingly mobile. Our dependency on mobile technology makes it an attractive and lucrative target for cyberattacks. A broad range of threats now challenges both government and consumer mobile devices. The government faces additional threats from advanced nation-state actors. Additionally, attacks can also focus on and jeopardize government employees' physical wellbeing, finances, or privacy. Moreover, a security compromise of a government employee's mobile systems can lead to unauthorized access to, change of, or destruction of government functions. To accelerate the safe and secure adoption of mobile technology within DHS and the federal government, the DHS S&T CSD created the Mobile Security R&D Program.

The following two presentations were quite relevant to the PSBN. The second one especially addressed one big challenge of the PSBN-ICAM where a device is shared among multiple users.

- **AI Underbrink:** presented a Security Information and Event Management (SIEM) system for Next-Generation Emergency response networks, which Correlate sensor data streams with network traffic to detect cyber threats.
- **QUO VANDIS** is a Framework for Mobile Device and User Authentication with the following highlights:
  - Device and User profiles can be transferred or shared among devices;
  - Policy Models using Location, Device Environment, Device Sensors, and User Input to establish trust.

## **A.7 Identity management**

This program investigates architectures, technical approaches, studies, processes, technologies, tools and proof-of-concepts across the following R&D topic areas:

- Authentication of people and non-person entities
- Risk based confirmation of identity that leads to trust

- Data and application security at rest and in transit
- Access control at the point of need
- User experience that incorporates security and privacy

The following two presentations were quite relevant to the PSBN and Broader security:

- Mobile device and attribute validation: provides Decentralized PKI, Attribute Certificates, which target First Responders and Broader users' applications to manage multiple attributes and provide tamper resistant storage in mobile devices.
- Emergency Responder Authentication System for Mobile Users: provides decentralized identity management and enrolls first responder mobile devices, enabling push notifications and enhanced security over home organization (i.e., password). It tracks skills and authorization and not just identity.

## **A.8 Other DHS S&T Divisions and Programs**

From our interactions with some of the DHS CSD Program managers, in addition to CSD and the First Responders Group (FRG), with whom we have already established a good relationship with, we have learned that DHS S&T has a few other divisions (parallel to CSD) that are very relevant to some of CSS' portfolios, which are worthwhile to explore further collaborations.

- Resilient Systems Division (RSD): RSD's mission is to rapidly develop and deliver innovative solutions that enhance the resilience of individuals, communities, and systems by enabling the Whole Community to prevent and protect against threats, mitigate hazards, effectively respond to disasters, and expedite recovery.
- Borders & Maritime Security Division (BMD) carries out research, development, test and evaluation activities to provide new or enhanced capabilities for maritime security, border and immigration enforcement and cargo supply chain security to DHS operational components.
- The Chemical and Biological Defense (CBD) Division works to increase the nation's preparedness against chemical and biological threats through improved threat awareness, advanced surveillance and detection, and responsive countermeasures. The division works with the Department of Homeland Security (DHS) component activities and other US government agencies to increase public and governmental awareness of potential chemical and biological threats and to strengthen the nation's response against these threats.
- Explosives Division (EXD) develops new technologies and systems to protect US citizens and infrastructure against the devastating effects of non-nuclear explosives, by seeking innovative approaches in detection and in countermeasures. The Division provides concepts, science, technologies, and systems that increase protection from explosives, and promotes the development of field equipment, technologies, and procedures to interdict weapons and explosive threats.

## Annex B Workshop agenda

Presentations can be obtained here:

<http://www.cvent.com/events/2017-cyber-security-r-d-showcase-and-technical-workshop/custom-35-9acde78a545049728c03bf3874f47532.aspx>.

*Table B.1: Workshop agenda.*

Tuesday, July, 11, 2017		
8:00AM	Registration Location: Grand Ballroom Promenade Foyer	
General Session		
9:00AM	<a href="#">Introductions/Welcome</a>	Douglas Maughan DHS S&T CSD Division Director
9:10AM	<a href="#">Keynote</a>	Rob Joyce White House Cyber Security Coordinator
9:40AM	CSD Strategic Vision	Douglas Maughan DHS S&T CSD Division Director
	Panel Discussion: Innovations in Cyber Security Education	
10:10AM	Panelists: Alice Hockenbury, Girl Scouts of the USA VP of Public Policy and Advocacy Kim Paradise, LifeJourney VP of Strategic Partnerships Russ Shilling, Digital Promise Global Senior Innovation Fellow	Moderator Edward Rhyne DHS S&T CSD Federated Security Program Manager
11:10AM	Morning Break	
11:25AM	Showcase	
	PROJECT	PRESENTER/AFFILIATION
11:25AM	<a href="#">Internet Atlas</a>	Paul Barford University of Wisconsin—Madison
11:45AM	<a href="#">Comic-Based Education and</a>	Laurin Buchanan

	<a href="#">Evaluation (Comic-BEE)</a>	Secure Decision
12:05PM	<a href="#">Self-Shielding Dynamic Network Architecture (SDNA)</a>	Nick Evancich Intelligent Automation Inc.
12:25PM	Lunch (on own)	
1:25PM	Showcase	
	PROJECT	PRESENTER/AFFILIATION
1:25PM	<a href="#">Mobile App Vetting</a>	Angelos Stavrou Kryptowire, LLC
1:45PM	<a href="#">Mapping Our Way to a More Secure Internet</a>	KC Claffy University of California San Diego
2:05PM	<a href="#">Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC)</a>	Robert Thorne BP
2:25PM	<a href="#">General Analysis Toolkit Using Record and Reply (GATOR)</a>	Julian Grizzard Johns Hopkins University Applied Physics Laboratory
2:45PM	Afternoon Break	
3:00PM	Showcase	
	PROJECT	PRESENTER/AFFILIATION
3:00PM	<a href="#">ZeroPoint</a>	Kevin Snow, ZeroPoint Dynamics
3:20PM	<a href="#">Security Controls Compliance Server</a>	Greg Elin GovReady
3:40PM	<a href="#">Securely Updating Automobiles</a>	Justin Cappos New York University
4:00PM	Closing Remarks for Day 1	Doug Maughan
4:05PM	Technology Demonstration / Poster Session Location: East, State and Palm Court Ballrooms	
Wednesday, July 12, 2017		
7:30AM	Registration Location: Grand Ballroom Promenade Foyer	
General Session		
8:30AM	<a href="#">Introductions/Updates</a>	Douglas Maughan DHS S&T CSD Division Director
8:40AM	<a href="#">Keynote</a>	TBD

[Panel Discussion: The CXO Fireside Chat: Threats, Challenges, Insights](#)

Panelists:













9:10AM Jerry Archer, SallieMae Chief Security Officer  
Alma Cole, CISSP, U.S. Customs and Border Protection Chief Information Security Officer (CISO)  
Robert Palmer, DHS Deputy Chief Technology Officer  
Michael Papay, Northrop Grumman CISO









Moderator: Vincent Sritapan  
DHS S&T CSD Mobile Security Program Manager

10:10AM Morning Break










Triple Technical Tracks

 New: 10 mins,  Middle: 15 mins,  Mature: 20 mins (includes 5 min Q&A)


Track 1	Track 2	Track 3
10:25AM-10:35AM <a href="#">SOFTWARE ASSURANCE PORTFOLIO OVERVIEW (SQA, SWAMP, ASTAM, STAMP)</a> PM Introduction: Kevin Greene	10:25AM-10:35AM <a href="#">SILICON VALLEY INNOVATION PROGRAM</a> PM Introduction: Melissa Ho	10:25AM-10:35AM <a href="#">MOBILE DEVICE SECURITY &amp; MOBILE APPLICATION SECURITY OVERVIEW (MDS)</a> PM Introduction: Vincent Sritapan
10:35AM-10:50AM  <a href="#">Reducing False-Positives in Software Quality Assurance Tools (SQA)</a> Adam Porter, University of Maryland	10:35AM-10:45AM  <a href="#">Internet of Things (IoT) Security</a> Bob Baxley, Bastille	10:35AM-10:55AM  <a href="#">Roots-of-Trust for Mobile Devices</a> Kris Carver, BlueRISC
10:50AM-11:00AM  <a href="#">Static Tool Analysis Modernization Project (STAMP)</a> Matthew Barry, Kestrel Technology	10:45AM-10:55AM  <a href="#">EndPoint-Detector: Normalized way to build novel IoT security solutions</a> Peter Jung & Kausik Sridharabalan, Pulzze Systems	10:55AM-11:15AM  <a href="#">Physical Unclonable Functions for Mobile Device Roots of Trust</a> Paul Rivera, Def-Logix
11:00AM-11:10AM  <a href="#">STAMPOut: Improving Software Security with Open-Source Static Analysis Tools</a> Dr. David Melski, GrammaTech	10:55AM-11:10AM  <a href="#">Blockchain Plugin to Make IOT Devices Tamper Proof</a> Tiana Laurence & Andrew Yashchuk, Factom	11:15AM-11:35AM  <a href="#">Virtual Mobile Infrastructure</a> Sanjay Challa, Hypori Federal
11:10AM-11:30AM  <a href="#">Software Assurance Marketplace (SWAMP)</a> Miron Livny, Morgridge Institute	11:10AM-11:25AM  <a href="#">IoT Security Suite</a> Geoff Barnard & William Bathurst, M2Mi	11:35AM-11:55AM  <a href="#">Trusted Monitor and Protection for Mobile Systems (TrustMS)</a> Guang Jin, Intelligent Automation,

for Research		Inc.
11:30AM-11:50AM  <a href="#">Hybrid Analysis Mapping</a> Dan Cornell, Denim Group	11:25AM-11:40AM  <a href="#">IoT Security Is Not a Myth</a> Allen Vance, Ionic	11:55AM-12:15PM  <a href="#">Multi-Modal Mobile Security Management for User Behavior Anomaly Detection and Risk Estimation</a> Ching-Yung Lin, IBM
11:50AM-12:10AM  <a href="#">Hybrid Application Security Testing</a> Ken Prole, Secure Decisions	11:40AM-11:50AM  <a href="#">IoT Secure Trust Anchor</a> Jonathan Butts, QED Secure Solutions	
12:10AM-12:20AM  <a href="#">A Real-Time Application Security Analyzer</a> Robert McGraw, RAM Laboratories, Inc.	11:50AM-12:00PM  <a href="#">Sexy Solutions to Old and Boring Problems</a> Ted Gudmundsen, Tamr	
	12:00PM-12:10PM  <a href="#">Moving Target Data Protection</a> Michael Burshteyn, CryptoMove	

12:20PM	Lunch (on own)
---------	----------------
















1:20PM-1:35PM  <a href="#">Application Security Threat Attack Modeling</a> Chris Horn, Secure Decisions	1:20PM-1:30PM  <a href="#">Radar Vision Platform for the Autonomous Era</a> Mo Hartney, Echodyne	1:20PM-1:40PM  <a href="#">Remote Access for Mobility via Virtual Micro Security Perimeters</a> Saman Zonouz, Rutgers University
1:35PM-1:50PM  <a href="#">Tools for Automated Detection and Assessment of Security Vulnerabilities in Mobile Applications</a> Sam Malek, George Mason University/University of California-Irvine	1:30PM-1:40PM  <a href="#">Operationalizing AI</a> Brian Losey, Shield AI	1:40PM-1:55PM  <a href="#">Neuromorphic and Early Warning Technology for Continuous Authentication of a Mobile Device</a> Vincent DeSapio, HRL Laboratories
1:50PM-1:55PM <a href="#">DISTRIBUTED DENIAL OF SERVICE DEFENSE (DDoSD)</a> PM Introduction: Ann Cox	1:40PM-2:25PM <a href="#">Panel Discussion: Venture Capitalists and Accelerators Believing in GovTech</a>	1:55PM-2:10PM  <a href="#">Theseus: A Security Information and Event Management System for Next-Generation Emergency Response Networks</a> AI Underbrink, Sentar, Inc.
1:55PM-2:10PM  <a href="#">Software Systems for Surveying</a>		2:10PM-2:25PM  <a href="#">QUO VANDIS: a Framework for</a>











[Spoofing Susceptibility](#)  
KC Claffy, University of California San Diego

2:10PM-2:35PM   
[DrawBridge: Leveraging Software-Defined Networking for DDoS Defense](#)  
Jun Li, University of Oregon

[Mobile Device and User Authentication](#)  
Tom Karygiannis, Kryptowire LLC

2:25PM Afternoon Break

2:40PM-2:55PM  <a href="#">NetBrane: a Software Defined DDoS Protection Platform for Internet Services</a> Christos Papadopoulos, Colorado State University	2:40PM-2:45PM <a href="#">INSIDER THREAT</a> PM Introduction: Megan Mahle	2:40PM-2:55PM  <a href="#">SENSEI: Sensor Secure Enterprise Infrastructure</a> Huy Nguyen, Metronom
2:55PM-3:10PM  <a href="#">DDoS Defense for a Community of Peers</a> Jem Berkes, Galois	2:45PM-3:00PM  <a href="#">Lightweight Media Forensics for Insider Threat Detection</a> Nicole Beebe, University of Texas San Antonio	2:55PM-3:00PM <a href="#">TRANSITION TO PRACTICE</a> PM Introduction: Nadia Carlsten
3:10PM-3:25PM  <a href="#">SENS: Security Service for the Internet</a> Jelena Mirkovic, University of Southern California Information Sciences Institute	3:00PM-3:05PM <a href="#">INTERNATIONAL PARTNERS</a> CSD Director Introduction: Doug Maughan	3:00PM-3:20PM  <a href="#">Dynamic Flow Isolation: Adaptive Access Control to Protect Networks</a> Rick Skowrya, Massachusetts Institute of Technology Lincoln Laboratory
3:25PM-3:40PM  <a href="#">The Software Defined Perimeter Solution for Bandwidth DDoS</a> Juanita Koilpillai, Waverley Labs	3:05PM-3:25PM  <a href="#">Two Aspects of Moving Target Defense Research Projects</a> Haim Zlatokrilov, Israeli National Cyber Directorate, Cyber Technologies Unit	3:20PM-3:40PM  <a href="#">APE: Android Intrusion Prevention for Android</a> Mark Mitchell, MITRE
3:40PM-3:55PM  <a href="#">Solving Complex Telephony Denial of Service, Robocall and Call Spoofing Attacks</a> Mark Collier, SecureLogix	3:25PM-3:45PM  <a href="#">Metrics and Mechanisms to Improve the Incentives for Cybersecurity</a> Carlos H. Gañán, Delft University of Technology	3:40PM-4:00PM  <a href="#">Keylime: Trust in the Cloud</a> Nabil Schear, Massachusetts Institute of Technology - Lincoln Laboratory
3:55PM-4:10PM  	3:45PM-4:05PM  	4:00PM-4:20PM  

<a href="#">Towards DDoS Resilient Emergency Dispatch Center</a> Weidong (Larry) Shi, University of Houston	<a href="#">Advanced Intelligent Anomaly Detection Systems for Cyber-Physical Systems</a> David Ong, Excel Marco Industrial Systems Pte Ltd.	<a href="#">Netowk FLOW AnalyzER (FLOWER)</a> Darren Curtis, Pacific Northwest National Laboratory
4:10PM-4:20PM <a href="#">CYBER APEX: NEXT GENERATION CYBER INFRASTRUCTURE</a> PM Introduction: Eric Harder/Greg Wigton	4:05PM-4:25PM  <a href="#">Strong Face Verification for Logon, Physical Access and Remote ID Verification</a> Andrew Bud, iProov	4:20PM-4:25PM <a href="#">CYBER RISK ECONOMICS (CyRiE)</a> PM Introduction: Erin Kenneally
4:20PM-4:30PM  <a href="#">Bringing Cybersecurity Solutions to the Financial Services Sector</a> Justin Taft, Cyber Apex Solutions	4:25PM-4:45PM  <a href="#">Shielding the Vulnerable Things</a> Sam Pickles, RedShield Security, Ltd	4:25PM-4:40PM  <a href="#">The Economics of Cybersecurity Research Data Sharing</a> Tyler Moore, The University of Tulsa
4:35PM-4:45PM  <a href="#">Increasing Attacker Cost When Targeting Financial Services Systems and Networks</a> Jonathan Ness, Veramine	4:45PM-4:50PM DETER TESTBED CSD Director Introduction: Doug Maughan	4:45PM-4:50PM  <a href="#">A New Paradigm in Risk Informed Cyber Insurance Policy Design: Meta-Policies and Risk Aggregation</a> Mingyan Liu, University of Michigan
4:40PM-5:00PM  <a href="#">Distributed Environment for Critical Infrastructure Decision-making Exercise (DECIDE)</a> Michael Schulz, Norwich University Applied Research Institute	4:50PM-5:10PM  <a href="#">Building Beyond DETER: Toward the Future of Cyber Experimentation with Advanced DETERLab Technologies</a> Terry Benzel, University of Southern California, Information Sciences Institute	4:50PM-5:10PM  <a href="#">FourSight-The Crowdsourced Cyber Threat Controls Benchmarking Information Marketplace</a> Mark Jaster, 418 Intelligence
		5:00PM-5:05PM CYBER RESILIENT ENERGERY DELIVERY CONSORTIUM (CREDC) & CRITICAL INFRASTRUCTURE RESLIENCE INSTITUTE (CIRI) PM Introduction: Erin Walsh
		5:05PM-5:25PM  <a href="#">CREDC &amp; CIRI</a> David Nicol, University of Illinois


Thursday, July 13, 2017

7:30AM Registration  
Location: Grand Ballroom Promenade Foyer














### Triple Technical Tracks










 New: 10 mins,  Middle: 15 mins,  Mature: 20 mins (includes 5 min Q&A)

Track 1	Track 2	Track 3
8:30AM-8:40AM <a href="#">INFORMATION MARKETPLACE FOR POLICY AND ANALYSIS OF CYBER-RISK &amp; TRUST (IMPACT)</a> PM Introduction: Erin Kenneally	8:30AM-8:35AM <a href="#">ANONYMOUS NETWORKS &amp; CURRENCIES</a> PM Introduction: Megan Mahle	8:30AM-8:35AM <a href="#">CYBER PHYSICAL SYSTEMS SECURITY</a> PM Introduction: Chase Garwood
8:40AM-9:00AM  <a href="#">Dimensions of Network Threat Intelligence</a> Paul Royal, Georgia Tech Information Security Center	8:35AM-8:50AM  <a href="#">Illuminating Onions—Known Onion Service Development and Tor Measurement</a> Rob Jansen, Naval Research Lab	8:35AM-8:50AM  <a href="#">Intrinsically Secure, Open and Safe Cyber-Physically Enabled, Life-Critical Essential Services (ISOSCELES) for Medical Devices</a> Todd Carpenter, Adventium Labs
9:00AM-9:20PM  <a href="#">Supporting Research and Development of Security Technologies through Network and Security Data Collection</a> KC Claffy, University of California San Diego	8:50AM-9:05AM  <a href="#">Exploring the Transition of Research-Derived Cyber Threat Data Sources</a> Phil Porras, SRI International	8:50AM-9:05AM  <a href="#">Secure Software Updates Over The Air (Uptane)</a> Sam Lauzon, University of Michigan Transportation Research Institute
9:20AM-9:40AM  <a href="#">Packets and Flows, Censuses and More</a> John Heidemann, Los Angeles/Colorado Research Exchange for Network Data	9:05AM-9:10AM <a href="#">CYBER FORENSICS</a> PM Introduction: Megan Mahle	9:05AM-9:20AM  <a href="#">Modeling Safety and Security Interactions in Buildings for Compositional Safety/Security Control</a> Xinming (Simon) Ou, University of South Florida
9:40AM-9:55AM  <a href="#">A Next Generation Repository for Sharing Sensitive Network and Security Data</a> Michael Kallitsis, University of Michigan	9:10AM-9:30AM  <a href="#">Cyber Forensics Support: National Software Reference Library, Computer Forensics Tool Testing, Computer Forensics Reference Dataset</a> Barbara Guttman, National Institutes of Standards and Technology	9:20AM-9:35AM  Side-Channel Causal Analysis for Design of Cyber-Physical Security David Payton, Hughes Research Lab
	9:30AM-9:45AM 	9:35AM-9:50AM 

<a href="#">A Supervised Learning Approach for Supplemental Malware Identification in Memory Images</a> DeMarcus Thomas, Mississippi State University	<a href="#">Medical Device Risk Assessment Platform: Community Driven Risk Transparency and Risk Reduction Across the Device Life Cycle</a> Dale Nordenberg, Medical Device Innovation, Safety and Security Consortium
9:45AM-9:55AM  <a href="#">Drone Forensics</a> Steve Watson, VTO Inc.	

10:55AM Morning Break

10:10AM-10:25AM  <a href="#">A Queryable 4Platform for Online Crime Repositories</a> Nicolas Christin, Carnegie Mellon University	10:10AM-10:20AM  Cyber Forensics New Award Performer TBD	10:10AM-10:25AM  <a href="#">Cyber Security for Vehicles</a> Kevin Harnett, Department of Transportation Volpe National Transportation Center
10:25AM-10:40AM  <a href="#">Digital Object Identifiers and the IMPACT Ecosystem</a> Ross Stapleton-Gray, Packet Clearing House	10:20AM-10:25AM <a href="#">IDENTITY MANAGEMENT</a> PM Introduction: Anil John	10:25AM-10:40AM  <a href="#">A Mission Impact Situational Awareness Tool for Distributed Operations Management of Cyber-Physical-Human Critical Infrastructures</a> Sean Warnick, Brigham Young University
10:40AM-10:45AM <a href="#">INTERNET MEASUREMENT AND ATTACK MODELING</a> PM Introduction: Ann Cox	10:25AM-10:45AM  <a href="#">Physical Access Control Using Derived Credentials Over NFC</a> Christopher Williams, Exponent & Kantara Initiative	10:40AM-10:55AM  <a href="#">High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Deployments</a> Manimaran Govindarasu, Iowa State University
10:45AM-11:05AM  <a href="#">Retro-Future Bridge and Outages</a> John Heidemann, University of Southern California Information Sciences Institute	10:45AM-11:00AM  <a href="#">Mobile Authentication Interoperability Using FIDO for Digital Certificates</a> Michael Queralt, Queralt	10:55AM-11:10AM  <a href="#">A Verifiable Framework for Cyber-Physical Attacks and Countermeasures in a Resilient Electric Power</a> Lalitha Sankar, Arizona State University
11:05AM-11:15AM  <a href="#">Situ/FASGuard</a> Joel W. Reed, Oak Ridge National	11:00AM-11:20AM  CASTRA: Context-Aware Security Technology for	11:10AM-11:25AM  <a href="#">Cyber-Physical Security for Advanced Manufacturing</a>



Laboratory	Responsive and Adaptive Protection Devu Manikantan Shila, United Technologies Research Corporation	Christopher Williams, Virginia Tech University
11:15AM-11:30AM  <a href="#">AI-Analyst: Cyberanalysis Workflow Acceleration</a> Sean Moore, Centripetal Networks	11:20AM-11:30AM  <a href="#">Device Super Identity</a> Glenn Fink, Pacific Northwest National Laboratory	11:25AM-11:35AM  <a href="#">SCADA Cyber Weakness in an AI-Enabled Cyber Training Platform</a> Kennan Skelly, Circadence Corp
11:30AM-11:45AM  <a href="#">Predictive Malware Defense</a> Avi Pfeffer, Charles River Analytics	11:30AM-11:45AM  <a href="#">Mobile Device and Attribute Validation</a> Steve Wilson, Lockstep Technologies & Kantara Initiative	11:35AM-11:45AM  <a href="#">Support for Security and Safety of Programmable IoT Systems</a> Darko Marinov, University of Illinois at Urbana-Champaign
11:45AM-12:05PM  <a href="#">Autonomous Detection and Healing of Silent Vulnerabilities</a> Jeff Gummeson, BlueRisc	11:45AM-12:00PM  <a href="#">Emergency Responder Authentication System for Mobile Users</a> Michael Schwartz, Gluu, Inc. & Kantara Initiative	11:45AM-11:55AM  <a href="#">Scalable Distributed Event and Intrusion Detection Systems (DEIDS) for Cyber Physical Power Systems</a> Drew Hamilton, Mississippi State University











12:00PM Lunch (on own)

## General Session


1:00PM	<a href="#">Keynote</a>	Dr. Edward Amoroso Founder & CEO, TAG Cyber LLC
1:40PM	Cyber Security Division Performer Awards & Conference Recap	Douglas Maughan DHS S&T CSD Division Director

2:00PM Transition Break

2:15PM-2:35PM  <a href="#">Securing Cyber-Physical Infrastructure with Symbiote</a> Nathaniel Boggs, Red Balloon	2:15PM-2:30PM  <a href="#">Match/ No Match Identity Validation Service</a> Steve Race, Transglobal Secure Collaboration Program	2:15PM-2:20PM <a href="#">FEDERATED SECURITY</a> PM Introduction: Ed Rhyne
---	--	--

2:35PM-2:50PM  <a href="#">Automatic Detection and Patching of Vulnerabilities in Embedded Systems</a> Carlos Roberto Aguayo Gonzalez, Power Fingerprinting	2:30PM-2:45PM  <a href="#">Composite Identity for High Assurance Remote Identity Proofing</a> David Fisher, CardSmart Technologies	2:20PM-2:40PM  <a href="#">The CipherRack Secure Tamper-Proof Cloud Platform</a> Radu Sion, Private Machines
2:50PM-3:00PM  <a href="#">Multi-Abstractions System Reasoning Infrastructure toward Achieving Adaptive Computing Systems</a> Michael McDougall, GrammaTech	2:45PM-3:00PM  <a href="#">Decentralized Key Management System Using Blockchain</a> Drummond Reed, Evernym	2:40PM-3:00PM  <a href="#">A Federated Command and Control Infrastructure</a> Tom Eskridge, Florida Institute of Technology
3:00PM-3:15PM  <a href="#">Trustbase</a> Daniel Zappala, Brigham Young University	3:00PM-3:15PM  <a href="#">Fit-for-Purpose Distributed Ledger (Blockchain) Technology</a> Manu Sporny, Digital Bazaar, Inc.	3:00PM-3:20PM  <a href="#">Moving Target Defense Reference Implementation</a> Andrew Mellinger, Carnegie Mellon University, Software Engineering Institute
3:15PM-3:30PM  <a href="#">Strengthening the Cyber Security of Critical Infrastructure through Discovery and Remediation of Vulnerable Supply Chain Organizations</a> April Lorenzen, DissectCyber	3:15PM-3:30PM  <a href="#">Digital Identity Leveraging Privacy-Enhancing Distributed Ledger Technology</a> Dmitry Barinov, Secure Key & DIACC	3:20PM-3:40PM  <a href="#">Secure Multi-Party Computation for Cyber Analytics</a> Emily Shen, Massachusetts Institute of Technology Lincoln Laboratory
3:30PM-3:45PM  <a href="#">Financial Sector Situational Awareness Part 1: Stock Markets</a> Scott Condie, Brigham Young University	3:30PM-3:35PM <a href="#">DATA PRIVACY</a> PM Introduction: Anil John	3:40PM-4:00PM  <a href="#">Cloud-COP: Cloud Computing Control Operations Plane</a> Aleksey Nogin, HRL Laboratories
	3:35PM-3:50PM  <a href="#">Privacy Preserving Federated Search and Sharing (PPFS2)</a> Shane Clark, Raytheon BBN Technologies	4:00PM-4:20PM  <a href="#">Moving Target Defense Technology Pilot</a> Vince Urias, Sandia National Labs
	3:50PM-4:00PM  <a href="#">Revealing and Controlling Privacy Leaks in Network Traffic</a> David Choffnes, Northeastern University	
	4:00PM-4:15PM  <a href="#">Differentially Private Anomaly Detection</a> Rebecca Wright, Rutgers	

University

4:15PM-4:30PM 

[A Platform for Contextual Mobile Privacy](#)

Dr. Nathan Good, Good Research

DOCUMENT CONTROL DATA		
*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive		
1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)  DRDC - Centre for Security Science Defence Research and Development Canada Carling Campus 60 Moodie Drive, building 7 Kanata ON K2H 8E9 Canada		2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)  CAN UNCLASSIFIED
		2b. CONTROLLED GOODS  NON-CONTROLLED GOODS DMC A
3. TITLE (The document title and sub-title as indicated on the title page.)  DHS S&T programs and cybersecurity showcase: Lessons learned and recommendations		
4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)  Tang, H.; Burman, R.		
5. DATE OF PUBLICATION (Month and year of publication of document.)  May 2018	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)  26	6b. NO. OF REFS (Total references cited.)  7
7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)  Reference Document		
8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)  DRDC - Centre for Security Science Defence Research and Development Canada Carling Campus 60 Moodie Drive, building 7 Kanata ON K2H 8E9 Canada		
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)	
10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)  DRDC-RDDC-2018-D045	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)	
11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)  Public release		
11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)		
12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)  public safety and security; cyber security		

13. ABSTRACT (When available in the document, the French version of the abstract must be included here.)

This report serves two purposes. The first is to summarize the highlights and lessons learned from the DHS Cybersecurity R&D Showcase and Technical Workshop (Cybersecurity Showcase in short). The second is to inform DRDC CSS program formulation by presenting the DHS S&T programs that are relevant to DRDC CSS and explore potential collaboration opportunities that can be leveraged with DHS S&T.

[Enter text: French]