DHS SCIENCE AND TECHNOLOGY

Cyber Security Division Overview and Silicon Valley Innovation Program

Homeland Security

Science and Technology

April 14, 2017

Douglas Maughan

Cyber Security Division Director

Agenda

- WDC Landscape and Recent R&D Plans
  - Federal R&D Strategic Plan
  - Critical Infrastructure Security and Resilience
  - National Privacy Research Strategy
- DHS S&T Cyber Security Division R&D Activities
  - Transition To Practice (TTP)
- Finance Sector Apex
- Silicon Valley Innovation Program (SVIP)

Federal Cybersecurity R&D Strategic Plan

- Requested by Congress in the *2014 Cybersecurity Enhancement Act* to update and expand the 2011 plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*
- Written in 2015 by an interagency working group for the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development Program (NITRD)
- Considered input from the President's Council of Advisors for Science and Technology (PCAST), an NSF RFI in May 2015, and DHS S&T community gatherings
- Released in February 2016 as a component of the President's National Cybersecurity Action Plan (CNAP)

Homeland Security
Science and Technology

National Critical Infrastructure Security and Resilience R&D

Homeland Security
Science and Technology

Erin Walsh, Ph.D.
Program Manager
Cyber Security Division
Homeland Security Advanced Research Projects Agency

Background

- In February 2013, President Obama issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21).
- President Obama also issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013.
- The coordinated release of these two policies underscored the commitment to integrating cyber and physical security and strengthening resilience across interrelated systems.
- Strengthening the Nation's critical infrastructure security and resilience is an ongoing priority for the Federal government.
- The functioning of the 16 critical infrastructure sectors is key to our economic, social, and national security.

PPD-21 Tasking

- PPD-21 replaced Homeland Security Presidential Directive-7 and directed the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan (NIPP)
  - Develop comprehensive research and development plan

Background

- DHS in coordination with OSTP and other Federal departments and agencies developed a National CISR R&D Plan "*that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments*."

- DHS' Science and Technology Directorate (S&T) was delegated lead responsibility for facilitating development of the National CISR R&D Plan through a collaborative, two-year process involving public and private stakeholders from across the critical infrastructure community.

- The Plan also establishes 10 R&D tenets, representing enabling principles for CISR R&D that apply across the critical infrastructure community.

- The Plan was released in November 2015. **http://go.usa.gov/cVXhj**

2015 National CISR R&D Priority Areas

A. Develop the **foundational understanding** of critical infrastructure **systems and systems dynamics**;

B. Develop **integrated and scalable risk assessment and management** approaches;

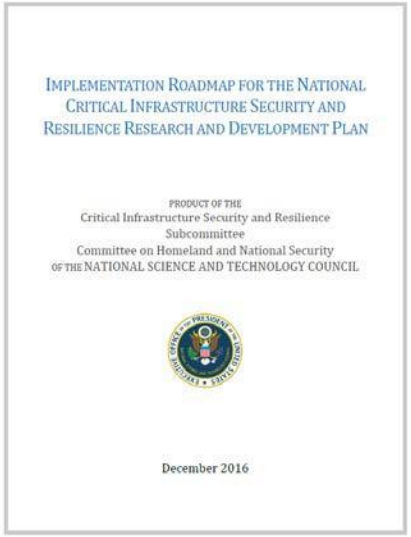
C. Develop **integrated and proactive capabilities, technologies, and methods** to support secure and resilient infrastructure;

D. Harness the power of data sciences to create **unified, integrated situational awareness** and to understand consequences of action;

E. Build a crosscutting culture of **CISR R&D collaboration**.

Federal Implementation

- PPD-21 required DHS to coordinate with OSTP and other Federal departments and agencies to align Federal R&D activities for CISR.
- The Federal CISR R&D community was convened in December 2015 through a subcommittee under the National Science and Technology Council.
- *Critical Infrastructure Security and Resilience (CISR) Research and Development (R&D) Implementation Roadmap* was published by OSTP in December 2016.



Implementation Roadmap Challenge Areas

1. Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making

2. Position, Navigation, and Timing Support Functions

3. Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems

4. Next-Generation Building Materials and Applications for Transportation Infrastructure Systems

5. Resilient and Secure Energy Delivery Systems

*Areas not explicitly covered in *The Federal Cybersecurity Research and Development Strategic Plan* (Feb. 2016) are addressed through specific activities in the *Implementation Roadmap*

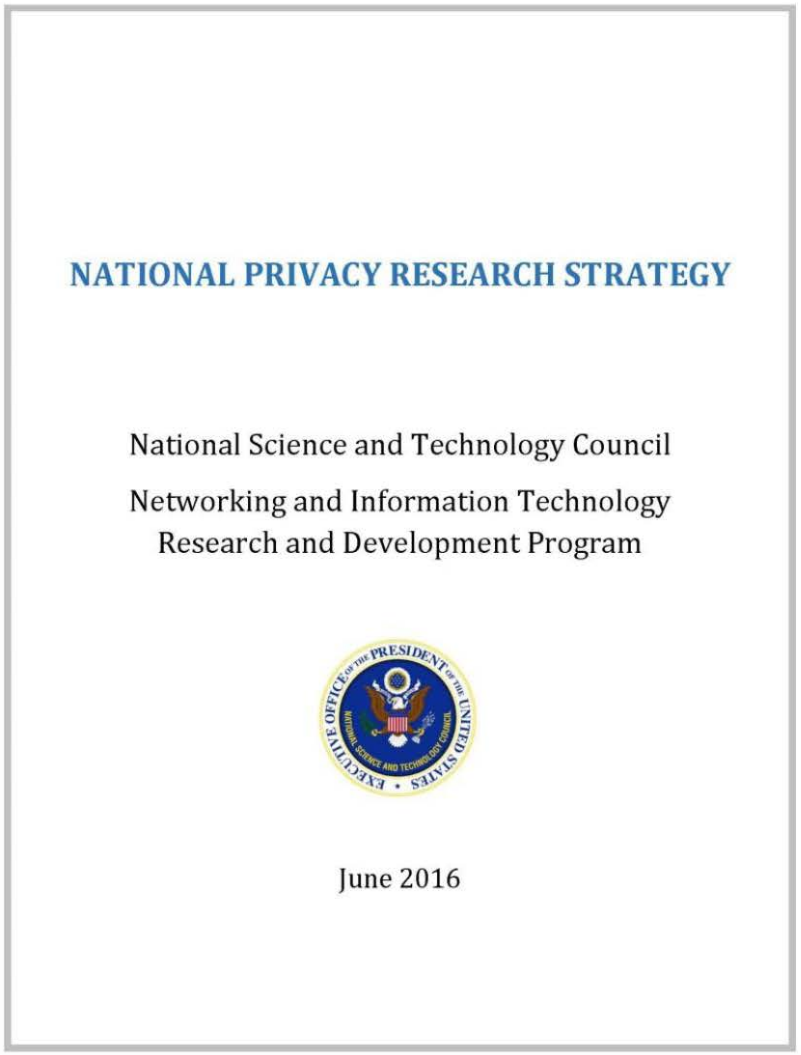
Table 1. CISR R&D Challenge Area Goals Mapped to National CISR R&D Priority Areas

Goal	Associated Priority Areas from CISR R&D National Plan (listed on p. 3)
Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making	
Models of Critical Infrastructure Interdependencies on Lifeline Functions	A, C, D
Data to Support Predictive Models and Decision Making	C, D, E
Effective and Efficient Decision Processes for Resource Allocation	C
Position, Navigation, and Timing Support Functions	
Technologies to Harden PNT Receivers	A, C
Technologies to Enable More Secure and Resilient PNT Services	A, C
Technologies to Enhance the Security of Current and Future PNT Systems	C
Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems	
Resilient Water and Wastewater Infrastructure	A, C
Methods and Strategies for Response to Disasters	B, C, D
Smart Water Systems for Water Resilience and Security	C
Next-Generation Building Materials and Applications for Transportation Infrastructure Systems	
Modernized Critical Transportation Infrastructure	C
Transportation Infrastructure to Withstand Extreme Events	C
More Rapid, Efficient and Cost-Effective Building and Repair of Transportation Infrastructure	A, C
Diagnostic Capabilities for Assessing the Performance and Condition of Infrastructure	C
Resilient and Secure Energy Delivery Systems	
System Design for Resilience	C, D
Preparedness and Mitigation Measures	B, C, E
Energy System Response and Recovery	C, E
Characterization and Management of Energy Interdependencies	B, C, E
Energy Systems that Withstand High-Impact, Low-Frequency Events	B, C
Develop Next-Generation Cybersecurity Capabilities	C

Dear Colleague Letter: Simulated and Synthetic Data for Infrastructure Modeling (SSDIM)

- Collaboration between NSF and DHS S&T to support research to develop and make available simulated and synthetic data on interdependent critical infrastructures (ICIs), and thus to improve understanding and performance of these systems.
- This DCL invites proposals for research that would contribute significantly to the scientific basis of simulated and synthetic data on ICIs.
- Proposals should address mechanistic and human aspects within at least two distinct critical infrastructures, along with interdependencies among them.
- Proposals may be submitted either as EAGER proposals or as requests for supplements to relevant NSF awards from the Directorate for Engineering and the Directorate for Computer and Information Science and Engineering by June 1, 2017.
- See **https://www.nsf.gov/pubs/2017/nsf17074/nsf17074.jsp**

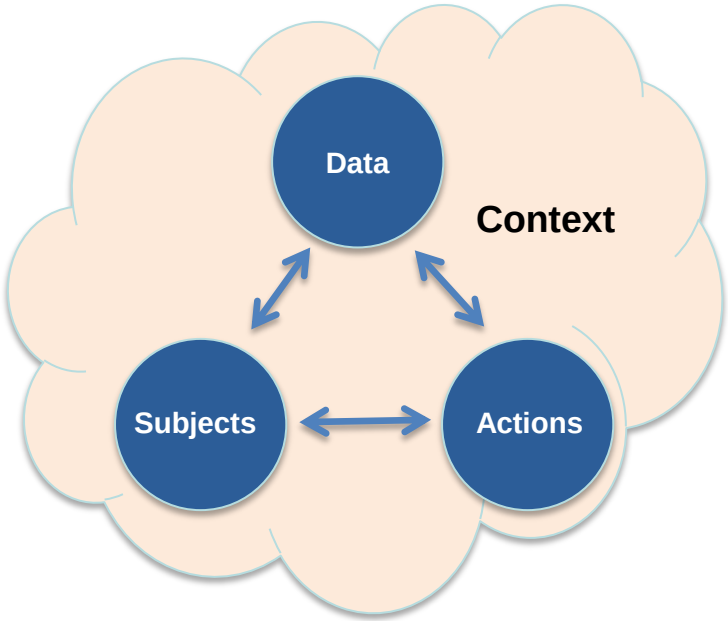
Federal Privacy R&D Priorities



https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf

Focus for Federal Privacy R&D

Privacy As



Role of Research

- Understand the nature of privacy
  - Privacy concerns solitude, confidentiality, the control of dissemination of personal information, the control of one's identity
  - Privacy is about the negotiation of personal spaces with those of peers, and with commercial and government entities
  - Privacy is contextual
- Understand privacy perspectives
  - Individual, Commerce, Government, Society
- Create knowledge and tools
  - To identify and mitigate emerging risks to privacy
  - To develop IT systems that can support privacy expectations and prevent unlawful discrimination, while supporting innovation

NITRD

Federal Priorities for Privacy Research

- Foster multidisciplinary approach to privacy research and solutions
- Understand and measure privacy desires and impacts
- Develop system design methods that incorporate privacy desires, requirements, and controls
- Increase transparency of data collection, sharing, use, and retention
- Assure that information flows and use are consistent with privacy rules
- Develop approaches for remediation and recovery
- Reduce privacy risks of analytical algorithms

NITRD

S&T MISSION

To deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise.

DHS and Cybersecurity

MISSION 4: SAFEGUARD AND SECURE CYBERSPACE

Goal 1: Strengthen the Security and Resilience of Critical Infrastructure

Goal 2: Secure the Federal Civilian Government Information Technology Enterprise

Goal 3: Advance Law Enforcement, Incident Response, and Reporting Capabilities

Goal 4: Strengthen the Ecosystem

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

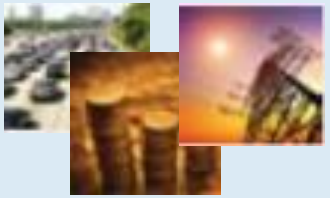
Research Requirement Inputs

WHITE HOUSE & NSS

DEPARTMENT INPUTS

INTERAGENCY COLLABORATIOIN

CYBERSECURITY



CRITICAL INFRASTRUCTURE SECTORS (PRIVATE SECTOR)

STATE & LOCAL

INTERNATIONAL PARTNERS

CSD Mission & Strategy

REQUIREMENTS





CSD MISSION

- **Develop and deliver new technologies, tools and techniques** to defend and secure current and future systems and networks
- Conduct and support **technology transition** efforts
- Provide **R&D leadership and coordination** within the government, academia, private sector and international cybersecurity community

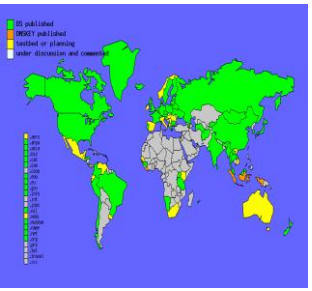
CSD PROGRAMS

- Cyber for Critical Infrastructure
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber Physical Systems
- Data Privacy Technologies
- Identity Management
- Homeland Security Open Source Technologies
- Human Aspects of Cyber Security
- Mobile Security
- Next Generation Cyber Infrastructure Ape
- Network System Security
- Research Infrastructure
- Software Assurance
- Transition to Practice

Homeland Security
Science and Technology

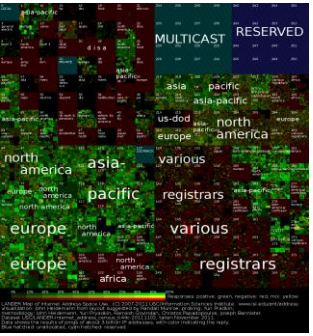
Trustworthy Cyber Infrastructure

Objective: Develop standards, policies, processes, and technologies to enable more secure and robust global cyber infrastructure and to identify components of greatest need of protection, applying analysis capabilities to predict and respond to cyber attack effects and provide situational understanding to providers



Secure Protocols

- Develop agreed-upon global infrastructure standards and solutions
- Working with IETF standards, routing vendors, global registries and ISPs
- Provide global Routing Public Key Infrastructure (RPKI) solutions
- Follow same process used for DNSSEC global deployment



Internet Measurement and Attack Modeling (IMAM)

- Create more complete view of the geographical and topological mapping of networks and systems
- Improve global peering, geo-location, and router level maps to assist automated solutions for attack prevention, detection, response
- Support cross-org, situational understanding at multiple time scales

Distributed Denial of Service Defenses (DDOSD)

- Policy-based technologies to shift the advantage to the defender
- Measurement/analysis tools to test success of BCP38 deployments
- Engaging with major finance sector companies and supporting ISPs

Homeland Security
Science and Technology

Research Infrastructure

Objective: Develop research infrastructure, such as test facilities, realistic datasets, tools, and methodologies to enable global cybersecurity R&D community researchers to perform at-scale experimentation on their emerging technologies with respect to system performance goals

DeterLab

Experimental Research Testbed (DETER)

- Researcher and vendor-neutral experimental infrastructure
- Used by 300+ organizations from 25+ states and 30+ countries - DARPA
- Used in 40 + classes, from 30 institutions and 3,000+ students
- Open Source code used by Canada, Israel, Australia, Singapore

Research Data Repository (IMPACT)

- Repository of over 1PB of network data for use by community
- More than 250 users (academia, industry, gov't – NSA SBIR)
- Leading activities on ICT Research Ethics (e.g., Menlo Report)
- Opening up to international partners (JP, CA, AU, UK, IL, NL)

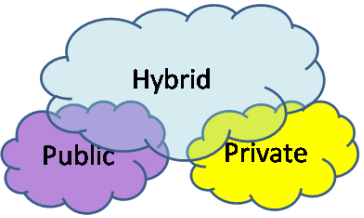
SWAMP

Software Assurance Market Place (SWAMP)

- A software assurance testing and evaluation facility and services
- Advance the quality and usage of SwA tools – commercial & open
- IOC – 2/1/14; 700+ assessments/week; 12 platforms; 10+ SwA tools

Network and System Security and Investigations - 1

Objective: Develop new and innovative methods, services, and capabilities for the security of future networks and systems to ensure they are usable and security properties can be measured and provide the tools and techniques needed for combatting cybercrime



Security for Cloud-Based Systems

- Develop methodologies and technologies for cloud auditing and forensics in end-point devices
- Identify data audit methodologies to identify the location, movement, and behavior of data and Virtual Machines (VMs)
- Work with DHS CIO/CISOs and datacenters

Mobile Device Security

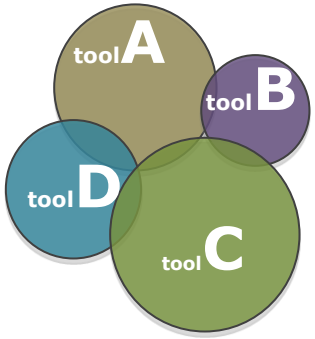
- Develop new approaches to mobile device security (user identity/authentication, device management, App security and management, and secure data) for government purposes
- Working with DHS CISO and across several components

Identity Management / Data Privacy

- Advance the identity management ecosystem to support Federal, state, local, and private sector identity management functions
- Develop data privacy technologies to better express, protect, and control the confidentiality of private information
- Working with DHS, other Federal, State, Local and Private Sector

Network and System Security and Investigations - 2

Objective: Develop new and innovative methods, services, and capabilities for the security of future networks and systems to ensure they are usable and security properties can be measured and provide the tools and techniques needed for combatting cybercrime



Software Quality Assurance

- Develop new methods and capabilities to analyze software and address the presence of internal flaws and vulnerabilities to reduce the risk and cost associated with software failures
- Develop automated capability to bring together independent software and system assessment activities

Usable Security and Security Metrics

- Improve the usability of cybersecurity technologies while maintaining security
- Develop security metrics and tools and techniques to make them practical and useful as decision aids for enterprise security posture

Investigation Capabilities for Law Enforcement

- Develop investigative tools/techniques for LE agencies to address the use of computers/phones in criminal and cyber related crimes
- Develop techniques and tools focused on detecting and limiting malicious behavior by untrustworthy insiders inside an organization
- Cyber Forensics Working Group – USSS, ICE, CBP, FBI, S/L

Cyber Physical Systems / Process Control Systems

Objective: Ensure necessary security enhancements are added to the design and implementation of ubiquitous cyber physical systems and process control systems, with an emphasis on transportation, emergency response, energy, and oil and gas systems.

Cyber Physical Systems Security (CPSSEC)

- Build security into the design of critical, smart, networked systems
- Gain better understanding of threats and system interactions
- Testing and validation of solutions in partnership with private sector
- Working with DoTrans and NPPD and Transportation Sector

Cyber Resilient Energy Delivery Consortium (CREDC)

- Improve the security of next-generation power grid infrastructure, making the underlying infrastructure more secure, reliable and safe
- 9 Universities and 2 national labs consortium – led by UIUC
- Private sector advisory board provides reqmts and transition path
- Partnership with DOE-OE and Universities

Securing the Oil and Gas Infrastructure (LOGIIC)

- Conduct collaborative RDT&E to identify and address sector-wide vulnerabilities in oil and gas industry digital control systems
- All R&D projects identified and funded by private sector members
- CSD provides project mgmt. support and inter-sector support

PRE-COMPETITIVE AUTOMOTIVE CYBERSECURITY RESEARCH

- Voluntary and technology-oriented Public-Private Partnership (PPP)
- Automotive OEMs with support from DHS S&T CSD, DOT-Volpe Center, and SRI International
- OEMs can pool resources and leverage them with government funding
- Cooperative “Pre-Competitive Research” (PCR) to improve the level of cybersecurity in automobiles
- Projects identified and selected by consortium members provide mutual benefit by reducing the threat of cybersecurity risks

Homeland Security
Science and Technology

The LOGIIC Model of Government and Industry Partnership

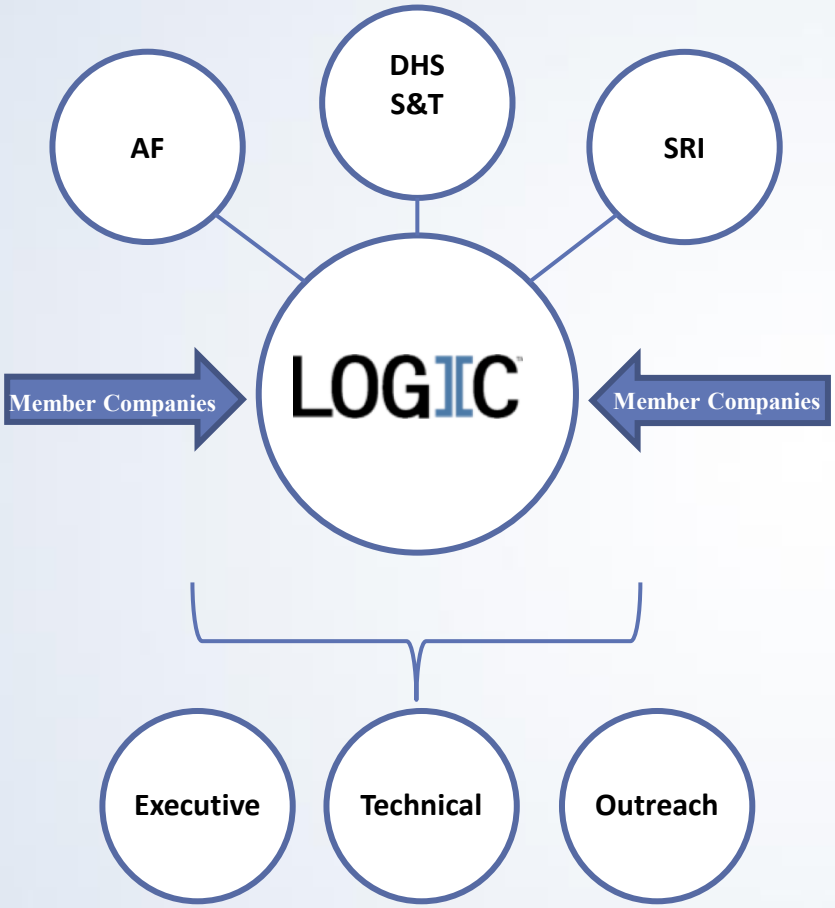
- **Linking the**
- **Oil and**
- **Gas**
- **Industry to**
- **Improve**
- **Cyber Security**

- LOGIIC is an ongoing collaboration of **oil and natural gas companies** and the **U.S. Department of Homeland Security, Science and Technology** Directorate (DHS S&T).
- LOGIIC facilitates cooperative research, development, **testing**, and evaluation procedures to **improve cyber security** in petroleum industry digital control systems.
- LOGIIC undertakes **collaborative research** and development projects to improve the level of cyber security.
- LOGIIC promotes the interests of the sector while **maintaining impartiality, the independence of the participants, and vendor neutrality.**

In 2012, **LOGIIC received the DHS S&T Under Secretary's Award for Outstanding Collaboration in Science and Technology**. LOGIIC has been commended by DHS S&T as a unique framework and a model for establishing similar consortia across other critical sectors.

Collaborative R&D

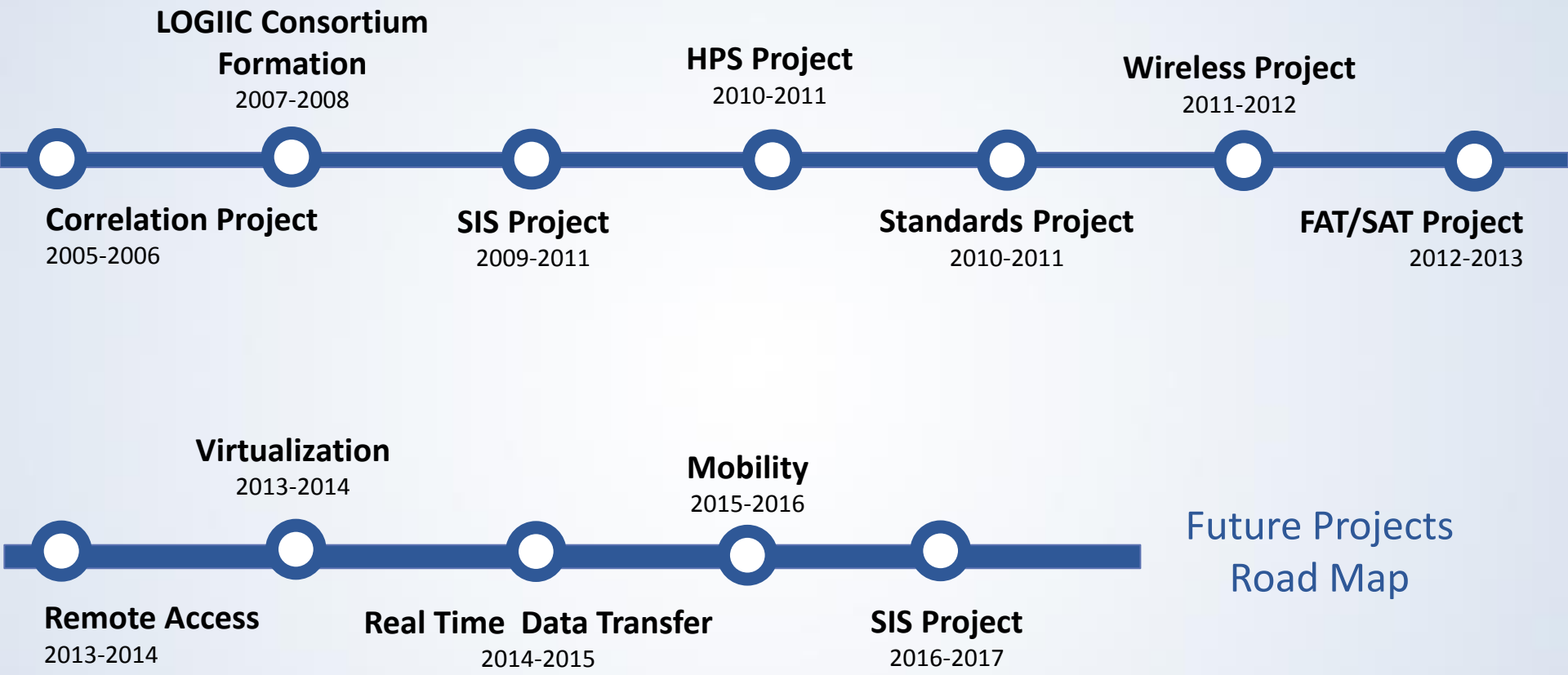
LOGIIC Broke New Ground in Consortium Governance



- The **Automation Federation** (AF) serves as the LOGIIC host organization.
- The U.S. **Department of Homeland Security**, Science and Technology Directorate has contracted with the scientific research organization SRI International to provide scientific and technical guidance for LOGIIC.
- Member companies contribute and provide staff to serve on the LOGIIC **Executive, Technical and Outreach Committees**. Current members of LOGIIC include **BP, Chevron, Shell, Total** and other large oil and gas companies that operate significant global energy infrastructure.

LOGIIC Projects Framework

LOGIIC Projects Timeline (2005 – 2015)



Future Projects Road Map

Public reports and presentations are available on the LOGIIC website

CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

CREDC Research Team

CREDC Research Areas

CREDC research develops tools and technology that improves cybersecurity on the operational technology (OT) side of energy delivery systems.

Research Theme Areas

- Cyber-protection Technology
- Cyber Monitoring, Metrics, and Evaluation
- Risk Assessment of EDS Technology and Systems
- Data Analytics for Cyber Event Detection, Management, Recovery
- Resilient EDS Architectures and Networks
- Impact of Disruptive Technologies on EDS
- Validation and Verification

Critical Infrastructure Resilience Institute

David M. Nicol
Franklin W. Woeltge Professor of Electrical and Computer Engineering University of Illinois
Director (ITI & CIRI)

www.ciri.illinois.edu

Resilient Critical Infrastructure

- Critical Infrastructures: Systems upon which our communities and lives depend, e.g.
  - Energy, water, transportation, communications, emergency services
- Resilience means
  - Ability to withstand (in part) upsetting event
  - Ability to deliver essential levels of service during upsetting event
  - Ability to recover quickly after upsetting event
- Resilience required at governance, business, community, physical infrastructure, and cyber infrastructure levels

Coverage of 9 DHS Sectors

Chemical

Commercial Facilities

Critical Manufacturing

Dams

Emergency Services

Government Facilities

Information Technology

Nuclear Reactors, Materials and Waste

Transportation Systems

Application Themes for CIRI

Insurance and Business Case for Resilience

- Find economic ways to spread risk, primarily in flood and cyber realms
- Technologies able to assess risk to standards acceptable by insurers
- Information sharing frameworks

Macro and Micro Industrial Supply Chains

- “micro” means intra-organization, “macro” means inter-organization
- Resilience issues in embedded systems
- Analysis of resiliency in business and policy context

Infrastructure Dependencies and Interdependencies

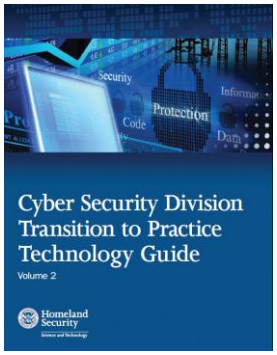
- “Situational awareness” of system dependencies/interdependencies
- Exploration of resilience governance issues
- Models of economic/social/physical impact of upsets

Communication

- Dependency of critical infrastructures on communication
- Mobile, Internet

Transition and Outreach

Objective: Accelerate the transition of mature federally-funded cybersecurity R&D technology into widespread operational deployment; Educate and train the current and next generations of cybersecurity workforce through multiple methods, models, and activities



Transition To Practice (TTP)

- White House initiated program in FY12; Over 30 technologies explored
- Working with DOE and DOD labs, FFRDCs, UARCs, NSF, SBIRs
- Leveraging over $250M in funding from other Federal Agencies
- Multiple pilots in progress; Multiple commercial licensing deals done

Cybersecurity Competitions

- Provide a controlled, competitive environment to assess a student's understanding and operational competency
- CSD-funded technologies included for test and evaluation
- 200+ schools and 2000+ college students participated in 2016
- Involvement from private sector; Assisting int'l competitions

National Initiative for Cybersecurity Education (NICE)

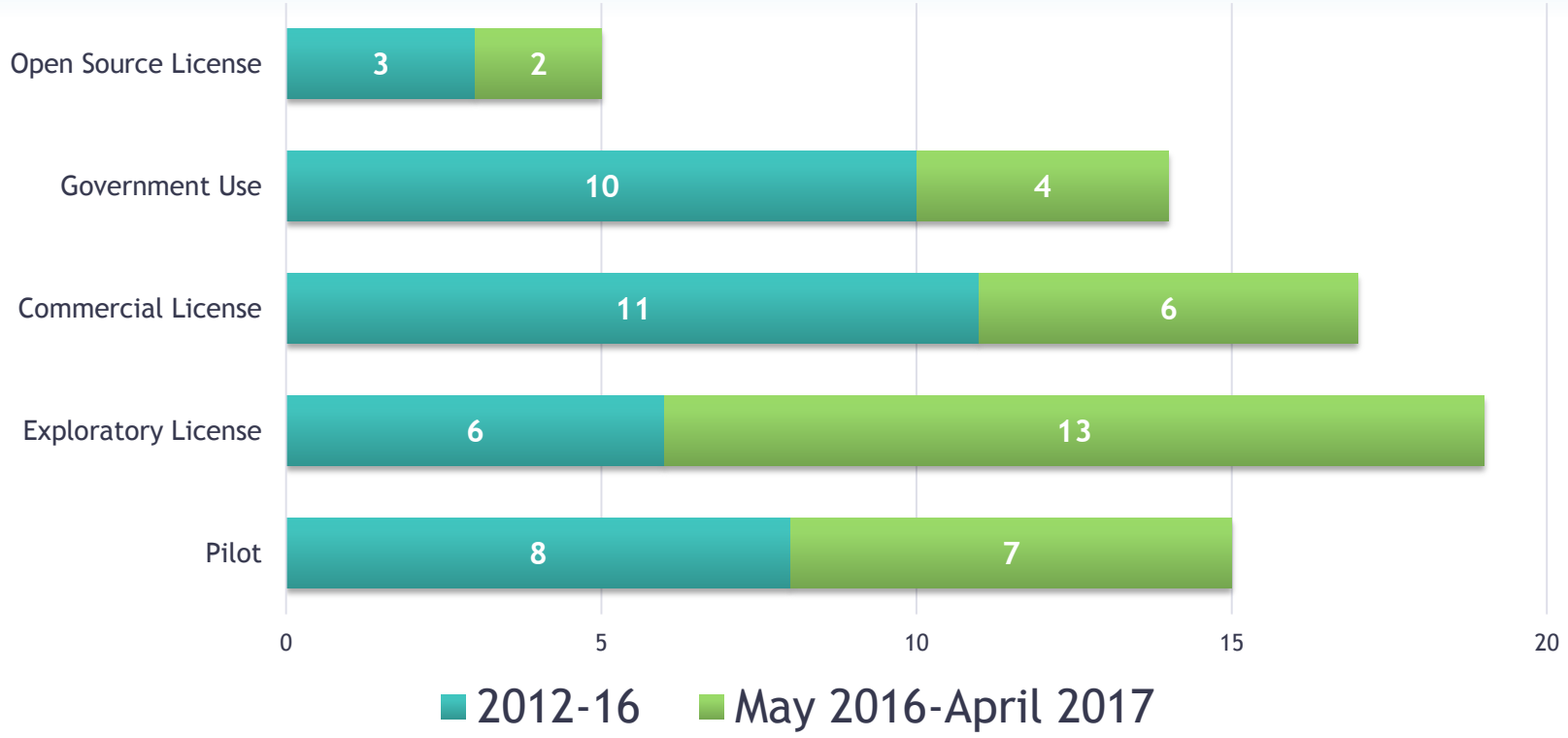
- Joint DHS/NSF/DOD/DOEd initiative with WH and NIST support
- Enhance Awareness (led by NPPD); Expand the Pipeline (led by CSD, NSF, DOEd); Evolve the Profession (led by NPPD and DOD)

Transition To Practice - Approach

R&D SOURCES	TTP PROCESS	UTILIZATION
DOE NATIONAL LABS	SELECTION	LICENSING
DOD LABS	TRAINING	STARTUPS
UARCs	MARKET VALIDATION	OPEN SOURCE
FFRDCs	TEST & EVALUATION	GOVERNMENT USE
ACADEMIA / NSF	PILOTS	ANALYSTS ADOPTION
	OUTREACH	
IAs with NSF, DOE…	MATURATION ACTIVITIES	MULTIPLE TRANSITION PATHS

Homeland Security
Science and Technology

Transition To Practice - Metrics



Homeland Security
Science and Technology

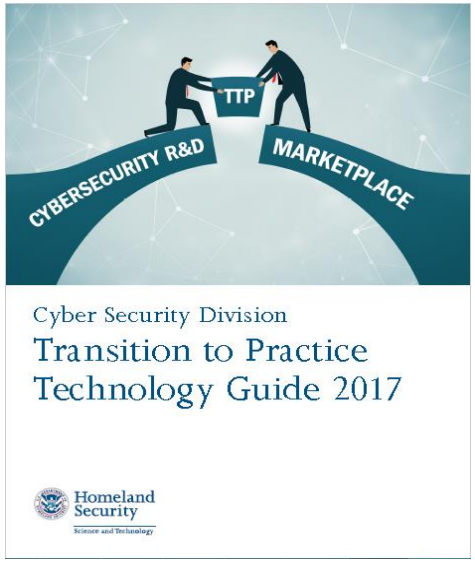
Transition To Practice - Successes

Project	Technology	Transition Path	Year	Outcome
Quantum Security	Entropy-as-a-Service platform	Commercialization	2015	Commercial product on market New company formed
Hyperion	Malware Forensics Detection and Software Assurance	Commercialization	2015	New company formed Commercial product on the market
Hone	Host and Network Data Correlation	Open Source	2015	Available for operational use
AMICO	Behavior Based Malware Downloads Detection	Open Source	2015	In use by universities
SCOT	Incident Response Threat Intel	Open Source	2015	In use by government
PathScan	Network Anomaly Detection	Commercialization	2016	Licensed by EY, integrated in services
NeMS	Network Characterization and Discovery	Commercialization	2016	New company raising capital
PACRAT	Vulnerability and Risk Analysis Tool	Commercialization	2016	Licensed, integrated into product
LOCKMA	Crypto Protection and Key Management	Licensed/Gov use	2016	In use by multiple agencies
CodeDNA	Malware identifier for community based defense	Government Use	2016	In use by DOD, US Cert
ZeroPoint	Weaponized Document detection	Commercialization	FY17	New security startup formed
PEACE	Policy Enforcement and Access Control for Endpoints	Commercialization	FY17	New security startup formed
PcapDB	Optimized Full Packet Capture	Open Source	FY17	Available for operational use
Keylime	TPM Based Trust in the Cloud	Open Source	FY17	Available for operational use

HAPPENING NEXT FOR TTP

- Investors, Integrators and IT Company (I3) Demo Days
- Demo Days for Critical Infrastructure
- Industry events
- Pilots

Engage With Us!



WEBSITE
dhs.gov/csd-ttp

EMAIL
ST.TTP@hq.dhs.gov

TWITTER
@dhsscitech
#TTPDemo

Save The Date!

TTP DEMO DAY 2017

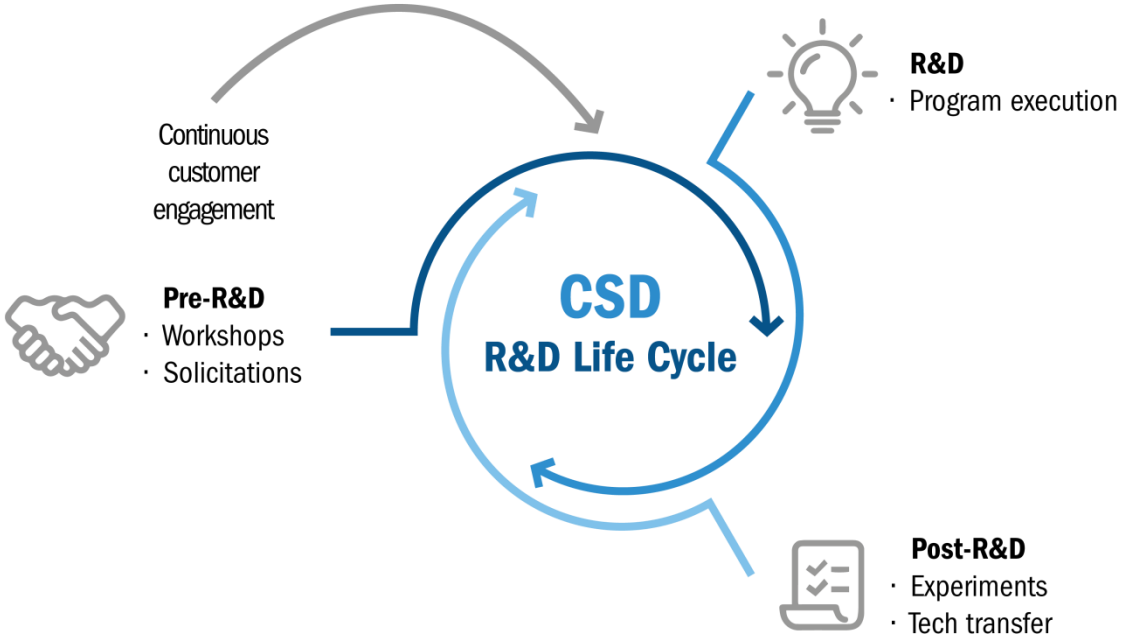
WHEN: Tuesday, May 16 2017

WHERE: Washington, DC

WHO: Cybersecurity professionals, technology investors, operators, and integrators

WHAT: Demo Day **featuring the new 2017 TTP cohort**. Discover eight new cyber technologies, see them in action, and collaborate with your cybersecurity colleagues!

CSD R&D Execution Model



"Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice,"
IEEE *Security & Privacy,* March-April 2013, Maughan, Douglas; Balenson, David; Lindqvist, Ulf; Tudor, Zachary
http://www.computer.org/portal/web/computingnow/securityandprivacy

Successes

Over 40 products transitioned since 2004, including:

- 2004 – BAA 04-17
  - 5 commercial products
  - 2 Open Source products
- 2005 – BAA 05-10 (RTAP)
  - 2 commercial products
  - 1 GOTS product
  - 1 Open Source product
- 2007 – BAA 07-09
  - 4 commercial products
- 2011 – BAA 11-02
  - 6 commercial products
  - 1 Open Source product
- BAAs – 2014, 2015, 2017
- Law Enforcement Support
  - 4 commercial products
  - 1 Open Source product
- Identity Management
  - 1 Open Source standard and GOTS solution
- SBIRs
  - 10+ commercial products
  - 2 Open Source product

Recent Pilots and Transitions
Highlight the Depth & Breadth of CSD R&D

Technology	Performer	Pilot or Transition Partner	Status
Cauldron Visualization Tool	GMU	CyVision Technologies	Commercialized
Net APT Firewall and Audit Analysis Tool	UIUC	Network Perceptions, primarily w/Energy Sector	Commercialized
Blackthorne GPS Forensics	Berla	ICE, USSS, CBP	Commercialized
Autonomy Forensics platform	Basis Technology	ICE, CBP, USSS	Commercialized
IVE Vehicle and Infotainment	Berla	ICE, CBP, DoD, State/Local, DoJ	Commercialized
Black Light Enhancements	Black Bag Forensics	US CERT, ICE, USSS, TSA, State/Local	Piloting - S&T funded licenses
NIST Forensics Tool Test Reports	NIST	Publically Available	Knowledge Products
Secure Network Attribution Prioritization Protocol	Raytheon	DoD/Army Cyber Command	Schoolhouse pilot and evaluation
Mobile Device Management	Mobile Iron	FEMA	Pilot and adoption by 10K users
Mobile App Security _ Mobile App vetting	Kryptowire	CBP, DHS HQ, US CERT	Pilot
Malware analysis tool	Hyperion	US CERT	Pilot
Hardware Enabled Zero Day Protection	Def-Logix	DoD/USAF	Pilot
Symbiote embedded device protection	Red Balloon Security	Hewlett Packard	Commercialized

Finance Sector Transition Project

Leverage existing federally funded and private sector research

- Integration, testing and evaluation
- Predominantly development

Establish the Cyber Apex Review Team (**CART**):

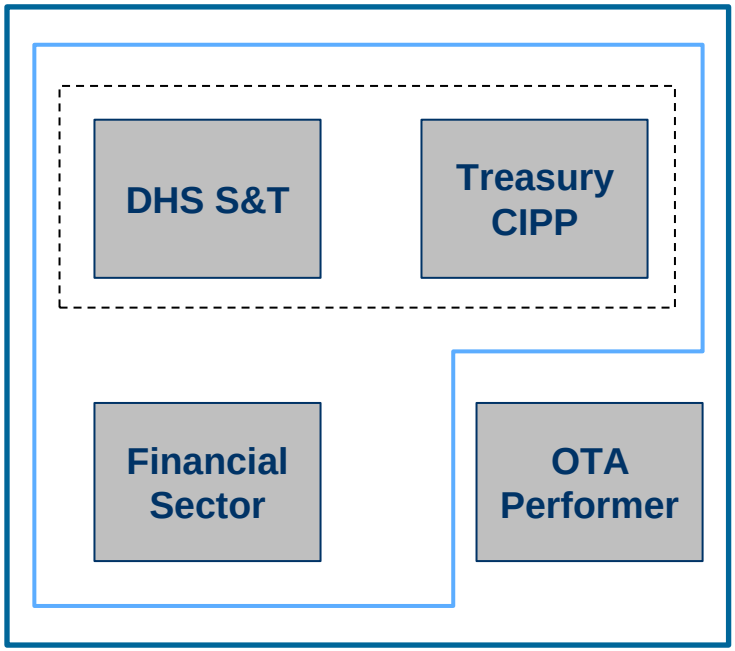
- DHS S&T + FS Critical Infrastructure + Treasury **partnership**
- Monthly meetings
- **Collaborate** on:
  - Sector needs and gaps identified (*relevance)* and ranked *(direction)*
  - **Common ontology** to join needs to technology areas
  - Task proposal evaluation

Execute via Other Transaction Authority (**OTA**)

- Adaptable **consortium** of performers
- Quick turn-around for task orders (*acceleration*)
- Flexible engagement with CART
- Iterate through the tech areas defined by CART

Apex Participant Levels:

- L_1: Government Only
- L_2: CART Members
- L_3: CART + OTA Performer



Functional Gaps and Technology

Impacts

Reduce Financial Sector risk due to cyber attack

Defend and deter cyber adversaries and limit the effect of cyber threats to information and operations

Functional Gaps

Identified by the Finance Sector **Subject to revision based on evolving requirements**

Software Assurance	Dynamic Defense	Network Characterization	Malware Detection	Insider Threat

Technology Areas

Hybrid Analysis	Visual Analytics	Zero Day Protection	Intrusion Tolerance	Dynamic Network Architecture	Network Mapping	Situational Understanding	Malware Classification	Malware Execution Prevention	Data Leakage

Leverage previous investments and existing technologies

- Over $60M in S&T funds invested in cyber security since 2010
- Over $20M in Government Lab funds invested in cyber security since 2010
- Private funding amounts as identified by the finance sector

Customer Buy-in

Active participation (June 2015 – present):

- Strategic Direction
  - Ranked capability needs mapped to technology areas, providing roadmap for task selection
- Technical Guidance
  - Technology and architecture surveys specific to FSS
- Initial tasks
  - NetAware: net situational awareness
  - NetIdentify: net structural awareness

Working with:

- Bob Blakley, Global Director for Information Security Innovation, Citigroup
- Byron Collie, Vice President, Threat Management, Goldman Sachs
- Ellen Moskowitz, Vice President, Corporate Information Security, State Street
- Parthiv Shah, SVP, CISO, The Clearing House
- George Smirnov, SVP, CISO, Comerica
- Sounil Yu, SVP, Director of R&D, Global Information Security, Bank of America

Homeland Security
Science and Technology

International Engagement

- “Cybersecurity is a global sport”
- This is not a U.S. only problem, everyone has the same problems; why not work on them together?
- Opportunities to leverage international funding for R&D and investment

VISION

- Joint Bilateral R&D Calls – Requires U.S. and Foreign researcher teams; initiated in FY17; first call in May 2017 with the Netherlands https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-17-R-B0001/listing.html
- Global Government Cybersecurity R&D Consortium – Similar to an existing First Responder consortium; forum for sharing R&D requirements to global entrepreneur and innovation communities. http://www.internationalresponderforum.org

Accelerating innovation for DHS and the homeland security enterprise to safeguard the American people, the homeland and our values.

Silicon Valley Innovation Program

What We Do

To keep pace with the innovation community and tackle the hardest problems faced by DHS's operational missions, we

EDUCATE

Help investors and entrepreneurs understand DHS's hard problems

FUND

Provide accelerated non-dilutive funding (up to $800K US) for product development to address DHS's needs

TEST

Provide test environments and pilot opportunities

What We Fund

Internet of Things Security

Background

Closed: Dec 2016

K9 Wearables

Open Application

Closes: June 2017

Big Data

Open Application

Closes: June 2017

Drones

Open Application

Closes: April 2017

Identity

Open Application

Closes: July 2017

Fintech Cybersecurity

Open Application

Closes: Nov 2017

https://scitech.dhs.gov/hsip

How We Fund

Potential for $800K; Up to 24 months

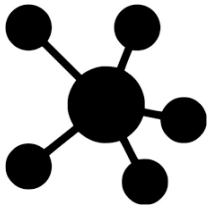
Performance-based funding steps			
Phase 1	**$50-200K**	**3-6 months**	**Proof of concept demo**
Phase 2	**$50-200K**	**3-6 months**	**Demo pilot-ready prototype**
Phase 3	**$50-200K**	**3-6 months**	**Pilot test prototype in operations**
Phase 4	**$50-200K**	**3-6 months**	**Test in various operational scenarios**

- Rolling applications reviewed approx. every 30 days
- If invited to pitch, funding decision made same day
- Contract awarded within 30-60 days

Why Us?

Equity-Free

This is a performance based contract. Up to $800K available for every company.



Network

Instant access to DHS public private partnerships and the greater homeland security enterprise, a $544B marketplace.

Mentorship

Learn from the best. We have a deep bench of government and private sector partners who can offer guidance and introductions.

Market Validation

Find market fit through prototype testing and pilot opportunities.

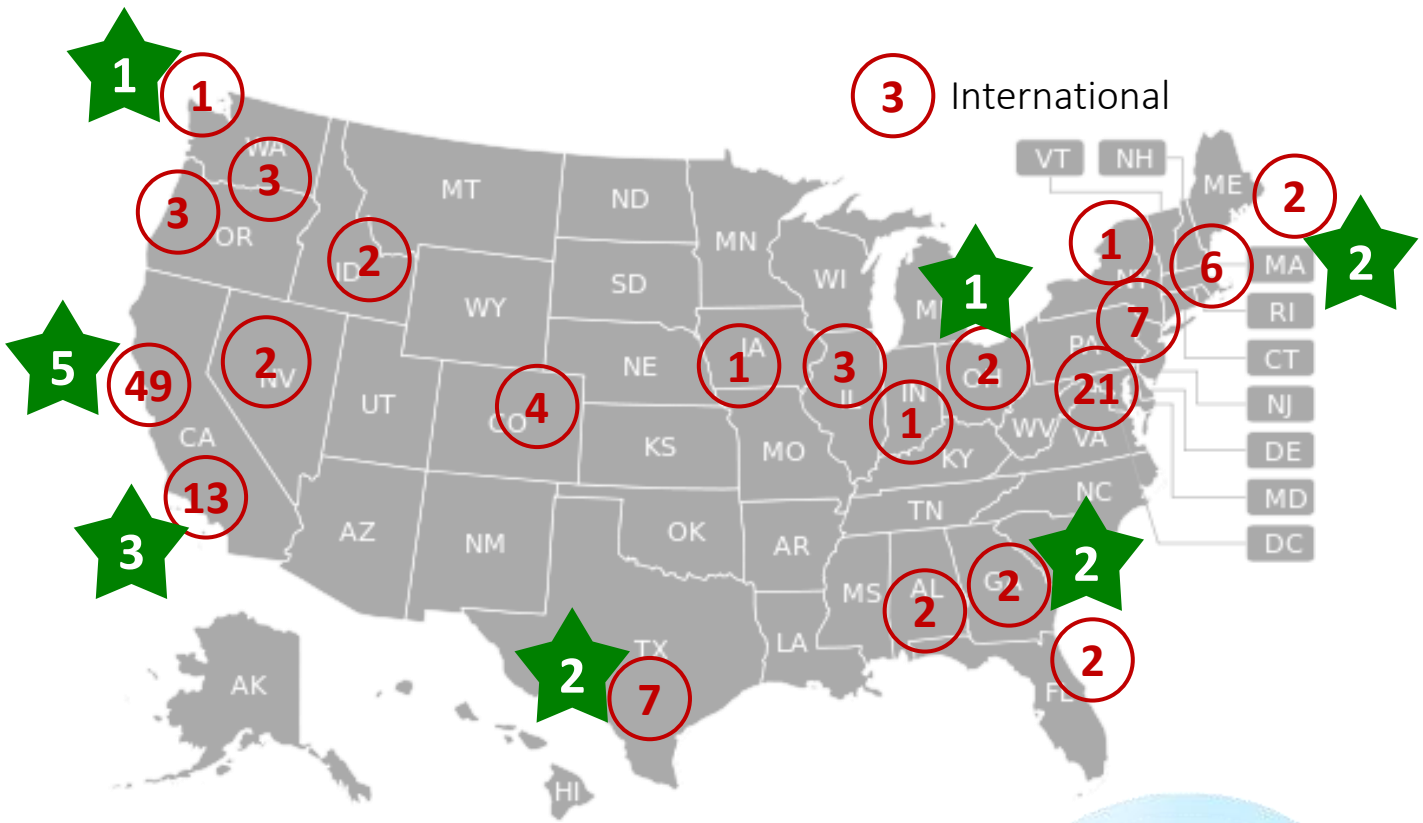
Amplify Your Reach

Demo your product to government, industry and investors from across the world.

Follow-On Funding

Our alumni have received follow-on funding by venture capital investors.

Latest Stats



6
Funded Topics

137
Applications

32
Pitches

16
Startups Funded

45
Days to Contract

Portfolio Companies

SVIP Funding Opportunity:
Financial Services Cyber Security Active Defense (FSCSAD)

Active (Dynamic) Defense: Present changing external and internal network layouts that are harder for adversaries to probe, breach and exploit, significantly increasing the economic costs for potential attackers

Three Technical Topic Areas:

- Intrusion Deception
- Moving Target Defense
- Isolation and Containment

Intrusion Deception

Cause adversary to believe in a falsehood in order to gain defensive advantage

Active deception:

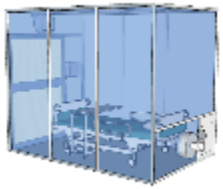
- Misdirect, frustrate, slow down, expose attackers or attack methodologies
- Target any phase of attack operations, e.g., reconnaissance, propagation, exploitation, command and control, data manipulation, exfiltration.
- Non-detectable by adversaries
- Focus on deception for networks, endpoints, applications, or data

Moving Target Defense (MTD)

Example Use Cases

- Self-modifying software services that randomly change binary program structure and memory use → turn vulnerability exploits into denial of service rather than permitting malicious code execution.
- Dynamic and random diversification of services (e.g., Microsoft IIS and Linux Apache) or host operating systems (Windows 10 and Ubuntu).
- Dynamic re-encryption of data.
- Dynamic re-distribution or movement of data

Isolation and Containment



Example Use Cases

- Force new software to execute in an isolated/contained environment to monitor for malicious activity prior to allowing it to execute in an enterprise environment.
- Execute all vulnerable services in isolation chambers so that if infected, the service cannot propagate within the enterprise.
- Isolate and monitor the activities of untrusted insiders to minimize any damage they could inflict on an enterprise.

Questions?

Email us | DHS-Silicon-Valley@hq.dhs.gov

Find us | https://scitech.dhs.gov/hsip

Follow us | **@dhsscitech #StartupDHS**

Summary / Conclusions

- Cybersecurity research is a key area of innovation to support our global economic and national security futures
- CSD continues with an aggressive cyber security research agenda to solve the cyber security problems of our current and future infrastructure and systems
  - Ever-increasing speed of technology change
  - Scope/complexity of the different areas of the problem
  - The balance of near-term versus longer-term R&D
- Will continue strong emphasis on technology transition
- Will impact cyber education, training, and awareness of our current and future cybersecurity workforce
- Will continue to work internationally to find and deploy the best ideas and solutions to real-world problems

Homeland Security

Science and Technology

Homeland Security
Science and Technology

Save The Dates!

2017 Cyber Security R&D Showcase and Technical Workshop

When: Week of July 10, 2017

What: Three days showcase and technical workshop

- 110+ technical presentations
- 40+ transition-ready technologies
- 50+ technology demonstrations
- Collaborate with 600+ cyber professionals from government, industry, academia and international partners

Visit dhs.gov/csd-events for more information.

Engage With Us!

WEBSITE
dhs.gov/cyber-research

PERISCOPE
www.periscope.tv/dhsscitech/

TWITTER
@dhsscitech

YOUTUBE
youtube.com/dhsscitech

FACEBOOK
@dhsscitech

S&T NATIONAL CONVERSATION
http://scitech.ideascale.com/

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

Douglas Maughan, Ph.D.

Division Director

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

For more information, visit

http://www.dhs.gov/cyber-research

CSD's Ten Strategic Visions

- International Engagement
- Secure Software
- Human Centric Cybersecurity
- Security of Mobile Computing
- Support for Law Enforcement
- Critical Infrastructure Security
- Measurement and Metrics
- Data Privacy
- Cybersecurity Education
- Technology Transition