DHS SCIENCE AND TECHNOLOGY

Re-inventing Cybersecurity R&D:
How DHS is Innovating to Deliver More Secure Systems

Homeland Security

Science and Technology

Doug Maughan

Cyber Security Division Director

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

STATE & LOCAL

CYBERSECURITY R&D

CRITICAL INFRASTRUCTURE SECTORS (PRIVATE SECTOR)

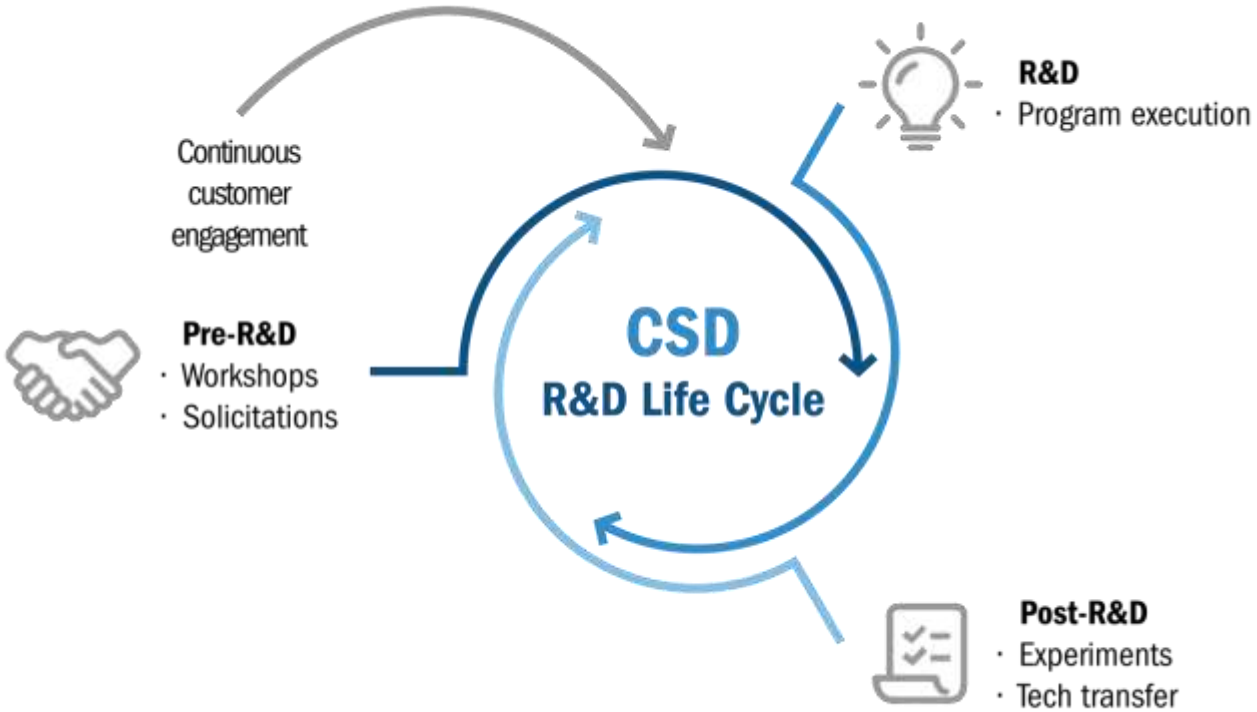
INTERNATIONAL PARTNERS

CSD Mission & Strategy

- Aviation Cybersecurity
- Cyber for Critical Infrastructure
- Cyber Physical Systems Security
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- Mobile Security
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- Silicon Valley Innovation Program
- Smart Cities
- Software Assurance
- Transition to Practice

- 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 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 75 technology products transitioned since 2004, including:

- 2004 – 2010
  - 11 commercial products
  - 3 Open Source products
  - 1 GOTS product
- 2011 – 2014
  - 12 commercial products
  - 3 Open Source products
  - 2 Knowledge products
- 2015 – 2018
  - 16 commercial products
  - 2 Open Source products
  - 3 Knowledge products
- Small Business Innovative Research (SBIRs)
  - 10+ commercial products
  - 2 Open Source products

Recent Transitions and Pilots

Technology	Performer	Pilot or Transition Partner	Status
Blackthorn GPS Forensics	Berla	ICE, USSS, CBP	Commercialized
iVe Vehicle and Infotainment Forensics	Berla	ICE, CBP, DoD, State/Local, DoJ	Commercialized
NIST Forensics Tool Test Reports	NIST	Publically Available	Knowledge Products
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
Policy Guru for TDOS Defense	SecureLogix	NG911, Banks, Hospitals	Three pilots

TTP Project	Technology	Transition Path	Outcome
PathScan (FY13 Cohort)	Network Anomaly Detection	Commercialization	Licensed by EY, integrated in services
NeMS (FY13 Cohort)	Network Characterization and Discovery	Commercialization	New company raising capital
CodeDNA (FY14 Cohort)	Malware identifier for community-based defense	Government Use	In use by DoD, US Cert
ZeroPoint (FY15 Cohort)	Weaponized Document detection	Commercialization	New security startup formed
PEACE (FY17 Cohort)	Policy Enforcement and Access Control for Endpoints	Commercialization	New security startup formed
PcapDB (FY16 Cohort)	Optimized Full Packet Capture	Open Source	Available for operational use
Keylime (FY17 Cohort)	TPM Based Trust in the Cloud	Open Source	Available for operational use

CSD Mission & Strategy

- Aviation Cybersecurity
- **Cyber for Critical Infrastructure**
- Cyber Physical Systems Security
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- Mobile Security
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- Silicon Valley Innovation Program
- Smart Cities
- Software Assurance
- Transition to Practice

- 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

The LOGIIC Model of Government and Industry Partnership

Linking the

Oil and

Gas

Industry to

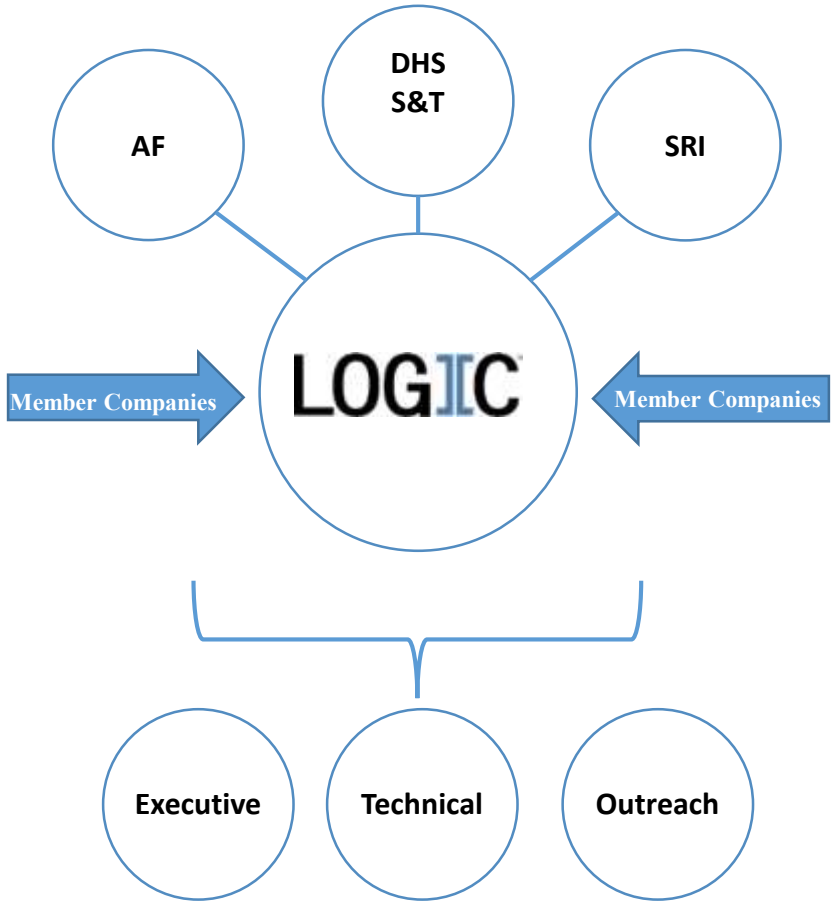
Improve

Cyber Security

- 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.**

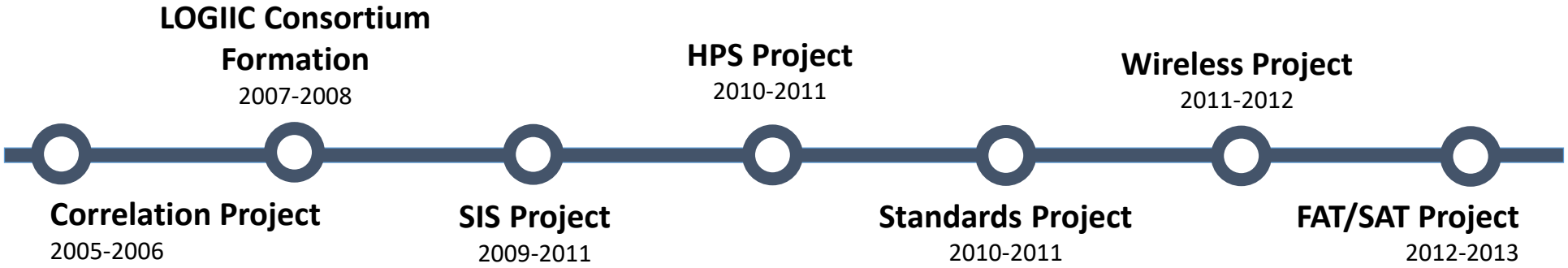
Collaborative R&D

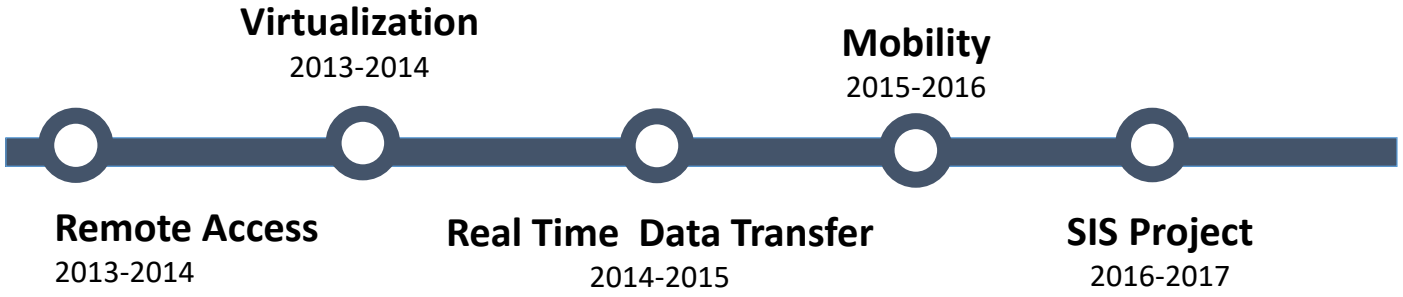
LOGIIC Broke New Ground in Consortium Governance



- The **Automation Federation** (AF) is 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, ExxonMobil, Shell, Total** and other large oil and gas companies that operate significant global energy infrastructure.

LOGIIC Projects Timeline (2005 – 2017)





Future Projects Road Map

https://www.dhs.gov/science-and-technology/csd-logiic

CSD Mission & Strategy

- Aviation Cybersecurity
- Cyber for Critical Infrastructure
- **Cyber Physical Systems Security**
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- Mobile Security
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- Silicon Valley Innovation Program
- Smart Cities
- Software Assurance
- Transition to Practice

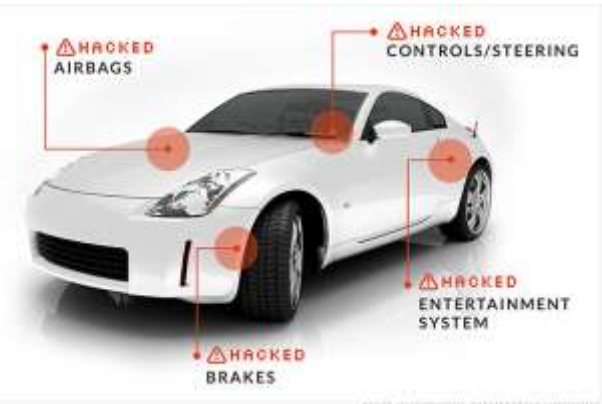
- Develop and deliver new technologies, tools and techniques to defend and secure current and future systems and networks
- Conduct and support technology transition efforts
- Provide R&D leadership and coordination within the government, academia, private sector and international cybersecurity community

CPS Security is Critical

- Smart cars, grids, medical devices, manufacturing, homes, smart everything!
- We bet our lives on these systems
  - cyber security ⇔ physical safety!
- Yet, CPS' are "cobbled together from stuff found on the Web"! (OK, there are good guys too)
- Who minds the shop?

Our lives

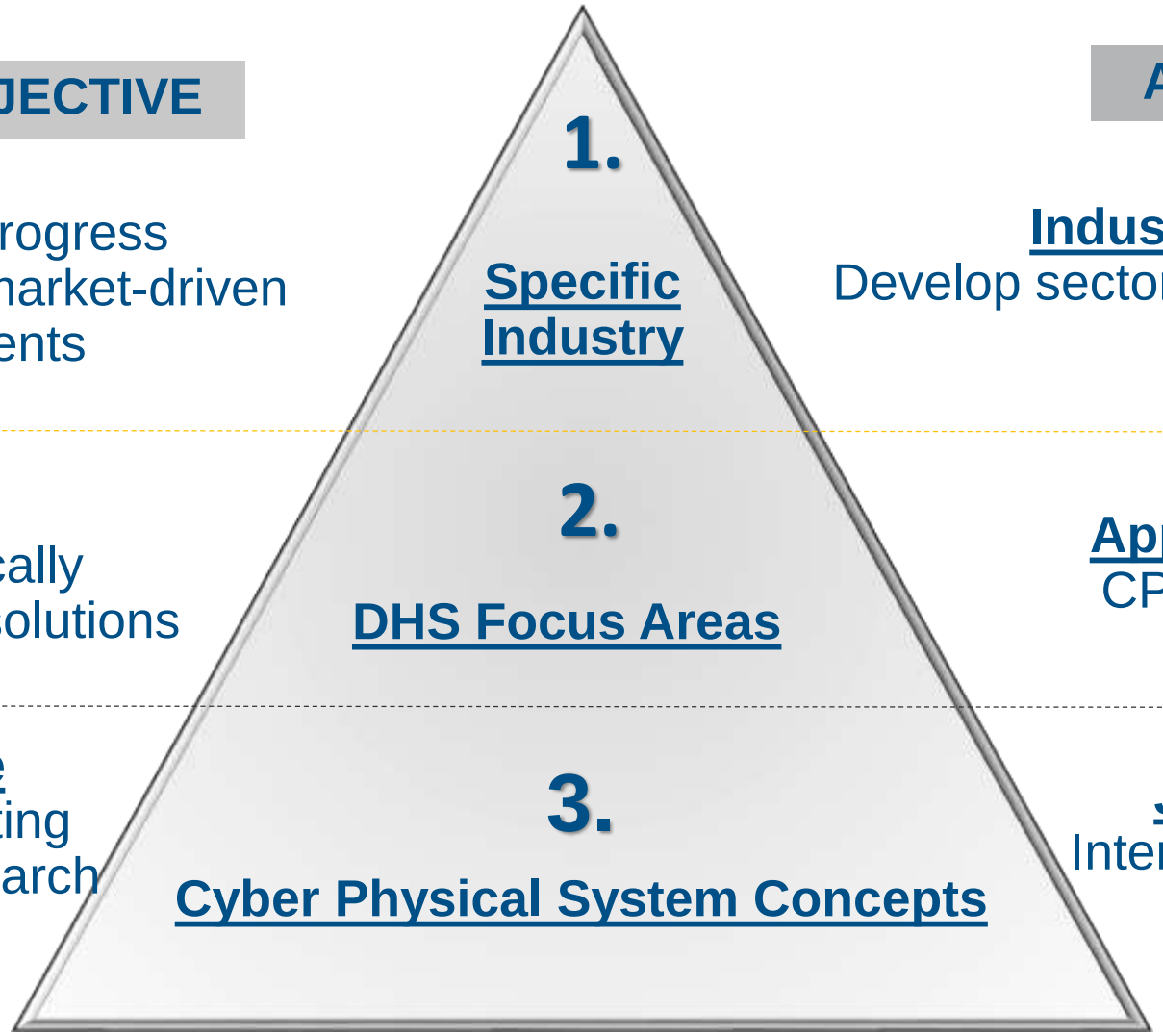
Our transport



Our stuff

Our health

S&T Program Structure



Example Focus Area: Vehicle Security

200M lines of code in a modern vehicle!

- **Telematics**
  - Remote control (locks, start)
  - Remote diagnostics
  - Remote repair (updates)

- **Driver support**
  - Navigation
  - Collision warning/avoidance
  - Augmented vision

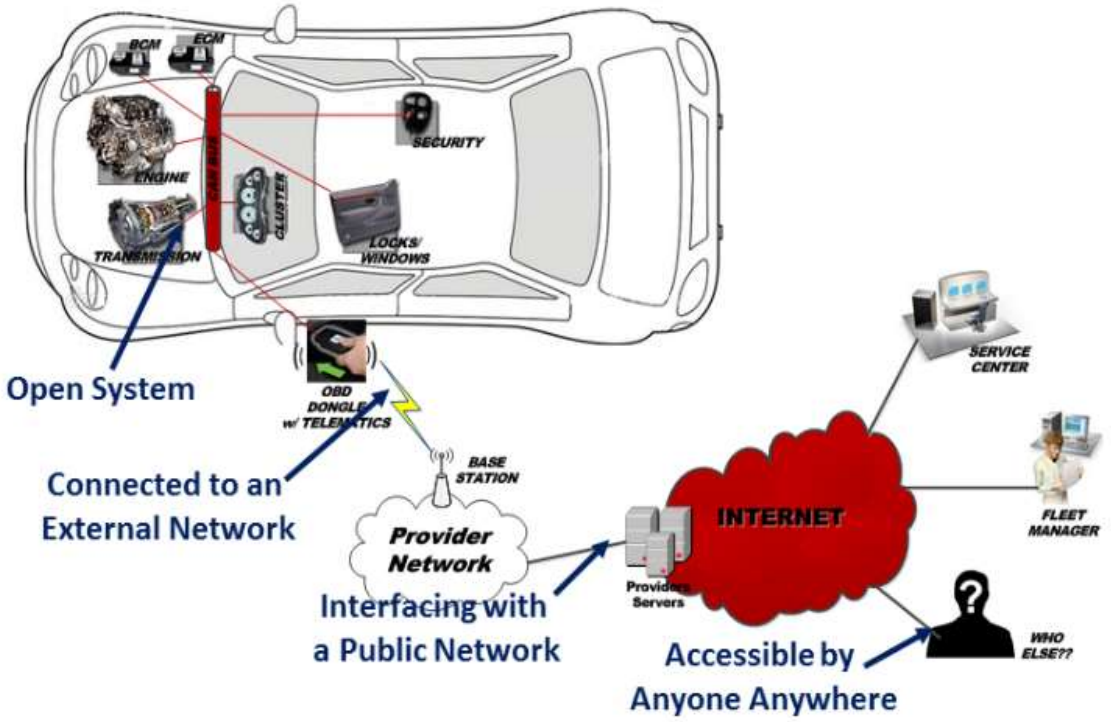
- **System automation**
  - Dynamic EV charging
  - Computer control of engine, brakes, etc.

- **Content and communication**
  - Voice and data
  - Information and entertainment

Automotive: Securing Telematics

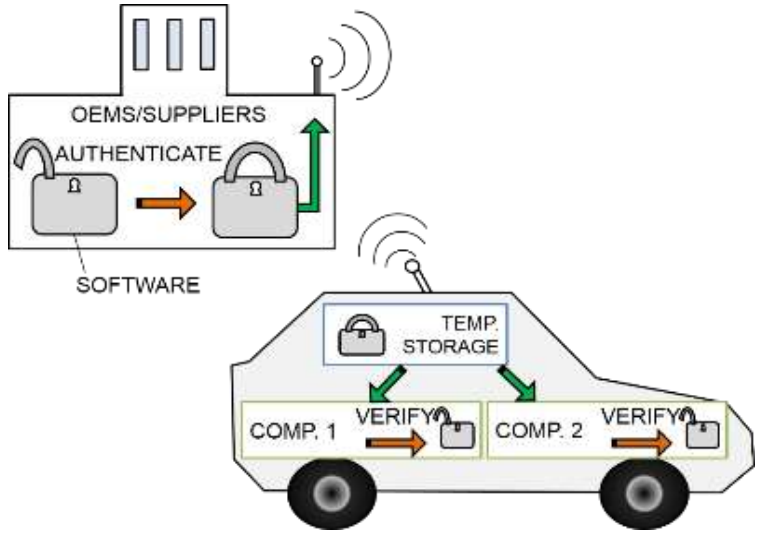
- **Problem -** Telematics needed to save fuel, reduce maintenance costs and for vehicle monitoring Although telematics has seen extensive use, security has not been a focus.
- **Solutions**
  - Telematics Cyber Security Primer for Agencies (to be made public)
  - Automotive Cybersecurity Industry Consortium (ACIC)

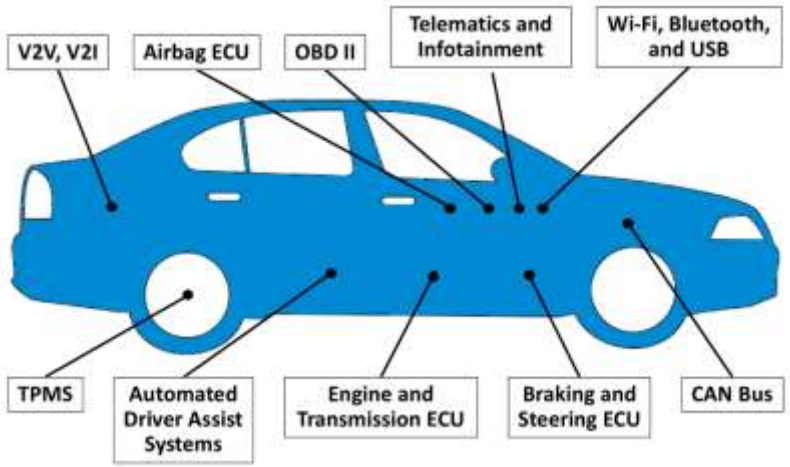
Performers – DHS S&T + DoT Volpe



Automotive: Software Updates

- **Problem** – Software-Over-the-Air (SOTA) updates are needed to rapidly correct critical flaws in vehicle software.
- **Solutions**
  - Uptane: a new generation of software updater that ensures separation of role with explicit/Implicit key revocation
  - mUptane: derivative implementation to solve compatibility concerns encountered by OEMs
- **Performers** – New York University (NYU) and University of Michigan Transportation Research Institute (UMTRI)





CSD Mission & Strategy

- Aviation Cybersecurity
- Cyber for Critical Infrastructure
- Cyber Physical Systems Security
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- **Mobile Security**
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- Silicon Valley Innovation Program
- Smart Cities
- Software Assurance
- Transition to Practice

- 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

Security of Mobile Computing

- Published "Study on Mobile Device Security"

(1) **Evolution of mobile security techniques from a desktop-centric** approach, and adequacy of these techniques to meet current mobile security challenges

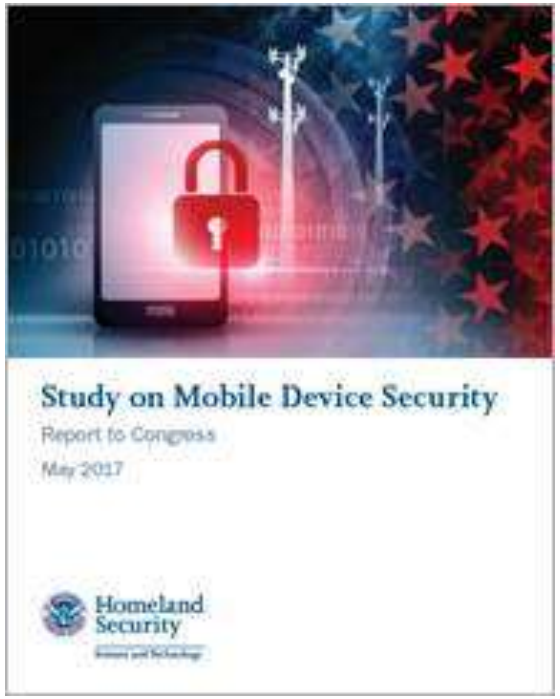
(2) **Effect** such threats may have **on the cybersecurity of the information systems and networks of the federal government**

(3) **Recommendations** for addressing the threats **based on industry standards and best practices**

(4) **Deficiencies in the current authorities of the Secretary** that may inhibit the ability of the Secretary to address mobile device security throughout the federal government

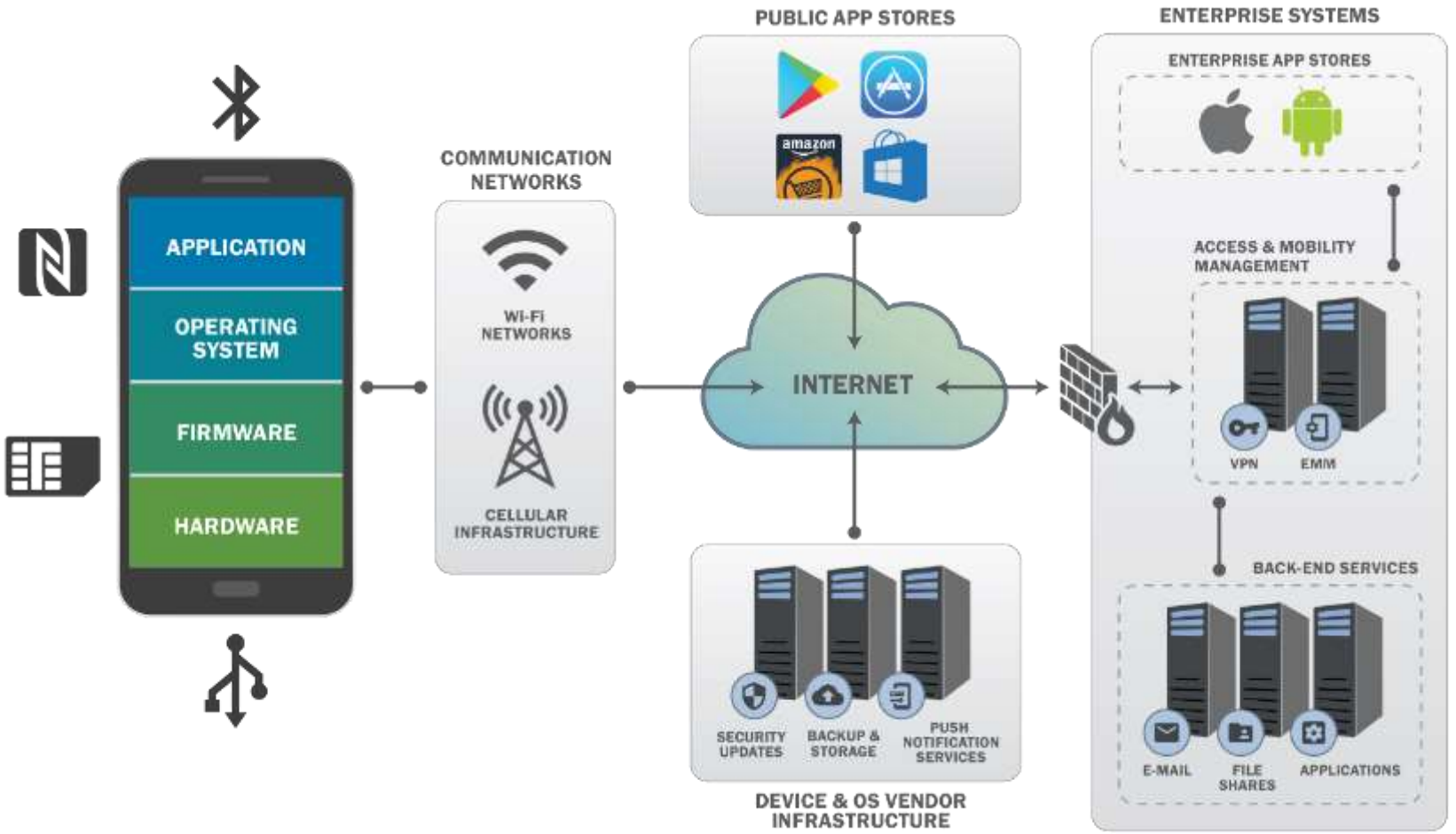
(5) **Plan for accelerated adoption** of secure mobile device technology by DHS

**Excludes National Security Systems and DoD and IC systems and networks*



https://www.dhs.gov/publication/csd-mobile-device-security-study

Mobile Ecosystem



Mobile Security Threats by Category

MOBILE DEVICE TECHNOLOGY STACK	• Delays in Security Updates • Exploitation of OS or Baseband Vulnerabilities • Deliberate Bootloader Exploitation • Jailbreak/Rooting • Supply Chain Compromise • TEE/Secure Enclave Exploitation • Compromised Cloud System Credentials
MOBILE NETWORKS	• Data/Voice Eavesdropping • Data/Voice Manipulation • Device and Identity Tracking • Denial of Service/Jamming • Rogue Base Stations & Wi-Fi Access Points • Interference with 911 Calls
DEVICE PHYSICAL SYSTEMS	• Device Loss or Theft • Physical Tampering • Malicious Charging Station • Attacks on Enterprise PCs
MOBILE APPLICATIONS	• Malicious and/or Privacy-Invasive Practices • Vulnerable Third-Party Libraries • Exploitation of Vulnerable App • Insecure App Development Practices • Exploit Public Mobile App Store • Malware, Ransomware
MOBILE ENTERPRISE	• Compromised EMM/MDM System or Admin Credentials • Man-in-the-Middle Attacks on Devices • EMM/MDM system impersonation • Compromised Enterprise Mobile App Store or Developer Credentials • Bypass App Vetting

Report Recommendations

- Threats to the government's use of mobile devices are real and exist across all elements of the mobile ecosystem.
- Recommend:
  - Adopt a framework for mobile device security based on existing standards and best practices.
  - Enhance Federal Information Security Modernization Act (FISMA) metrics to focus on securing mobile devices, applications, and network infrastructure.
  - Include mobility within the Continuous Diagnostics and Mitigation program to address the security of mobile devices and applications with capabilities that are at parity with other network devices (e.g., workstations and servers).
  - Several other recommendations, including R&D

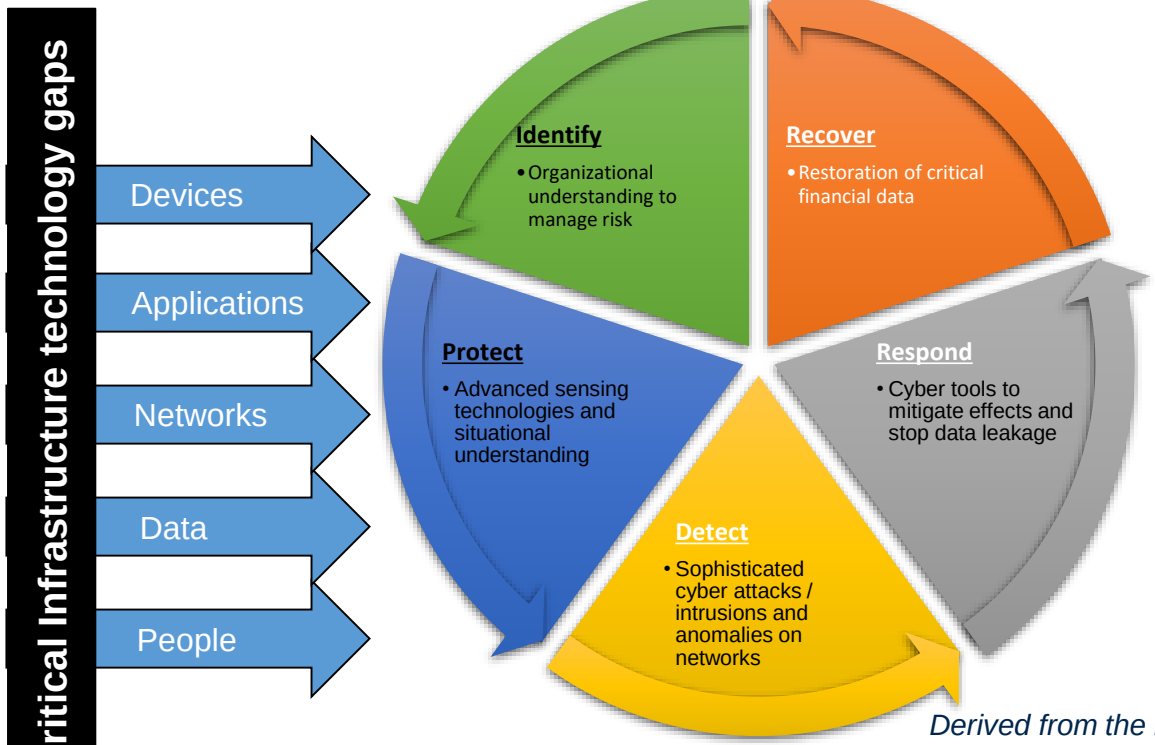
CSD Mission & Strategy

- Aviation Cybersecurity
- Cyber for Critical Infrastructure
- Cyber Physical Systems Security
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- Mobile Security
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- Silicon Valley Innovation Program
- Smart Cities
- Software Assurance
- Transition to Practice

- 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

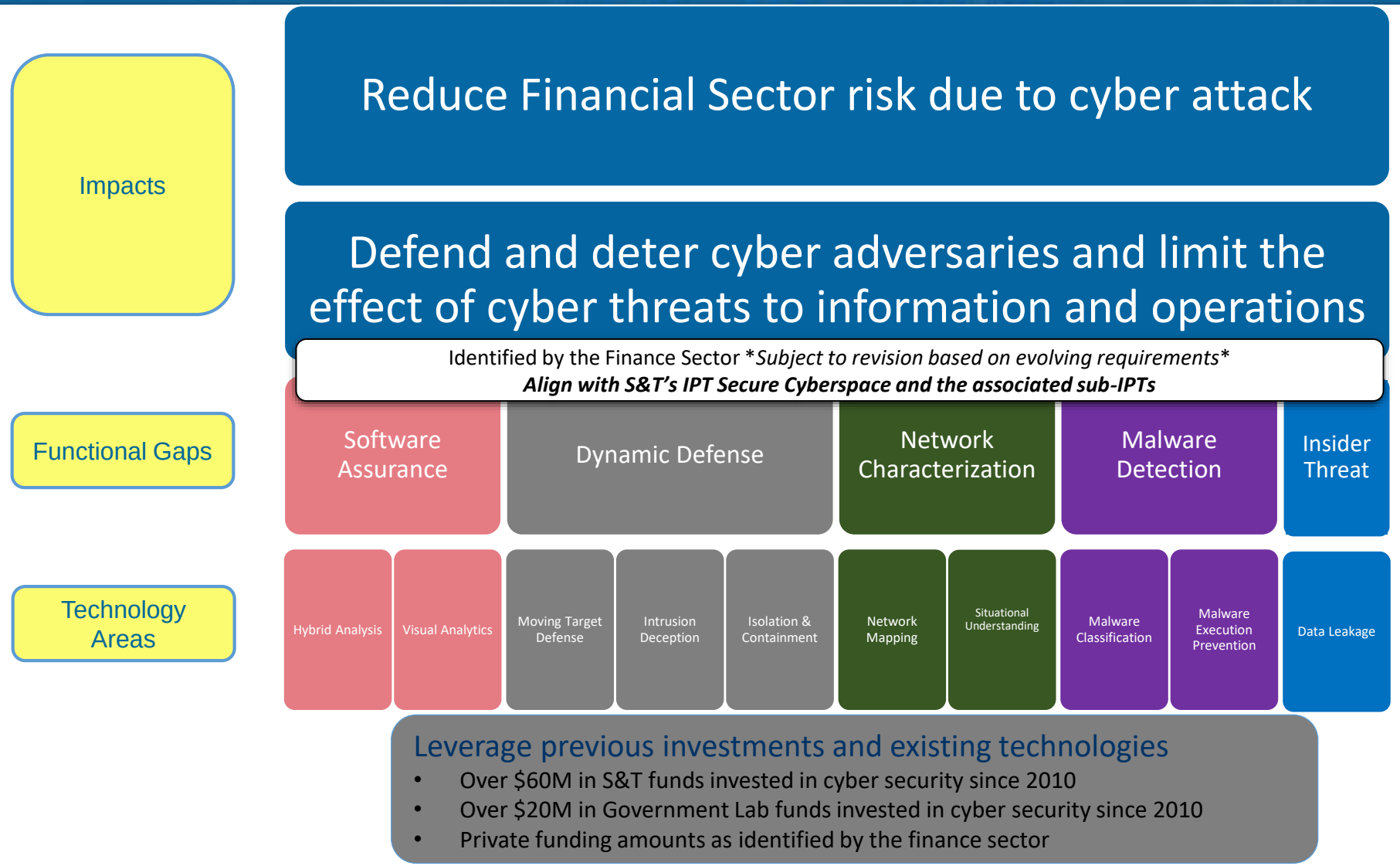
Next Generation Cyber Infrastructure (NGCI) Apex "Cyber Apex"

Partner with financial sector critical infrastructure to develop and integrate technologies that fill cyber technology gaps, resulting in a reduction of risk through the improvement of security.



Derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.0.

Finance Sector Technical Gaps and Technology



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

Stakeholder Engagement / Organization Chart

The program relies on participation from the Government, including DHS S&T and the Department of Treasury, the Financial Sector, and the Cyber Apex Consortium performer and Cyber Apex SVIP performers.

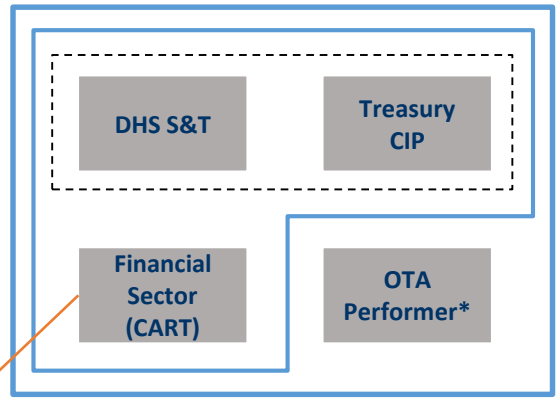
Ultimate decision making authority resides with the government based on inputs from the CART (includes Financial Sector).

https://www.dhs.gov/science-and-technology/customer-and-stakeholder-engagement

Financial Sector Participants Include

Apex Participant Levels:

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



CART prioritizes technology areas for the financial sector:

- Identifies cyber threats that plague the industry
- Ranks capability needs mapped to technology areas
- Provides roadmap, project selection guidance

CSD Mission & Strategy

- Aviation Cybersecurity
- Cyber for Critical Infrastructure
- Cyber Physical Systems Security
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- Mobile Security
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- Silicon Valley Innovation Program
- **Smart Cities**
- Software Assurance
- Transition to Practice

- 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

Smart Cities Team Challenge

GLOBAL CITY TEAMS CHALLENGE

110 Project Teams
160 Cities
400 Companies, Universities

SuperClusters

Intelligent Transportation

Energy, Water Waste Mgmt

City Platform Dashboard

Public Safety

Wireless Broadband

Data Governance & Exchange

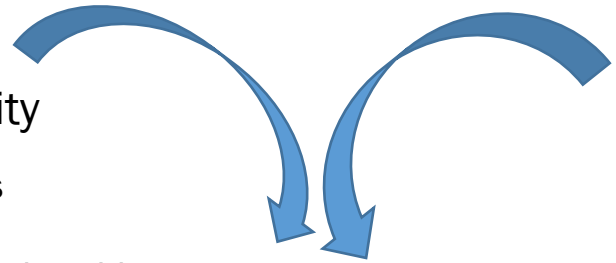
Rural Agriculture

DHS S&T and NIST Partnership

NIST

NIST
GCTC Community

110 Project Teams
160 Cities
400 Companies, Universities



DHS S&T
Community

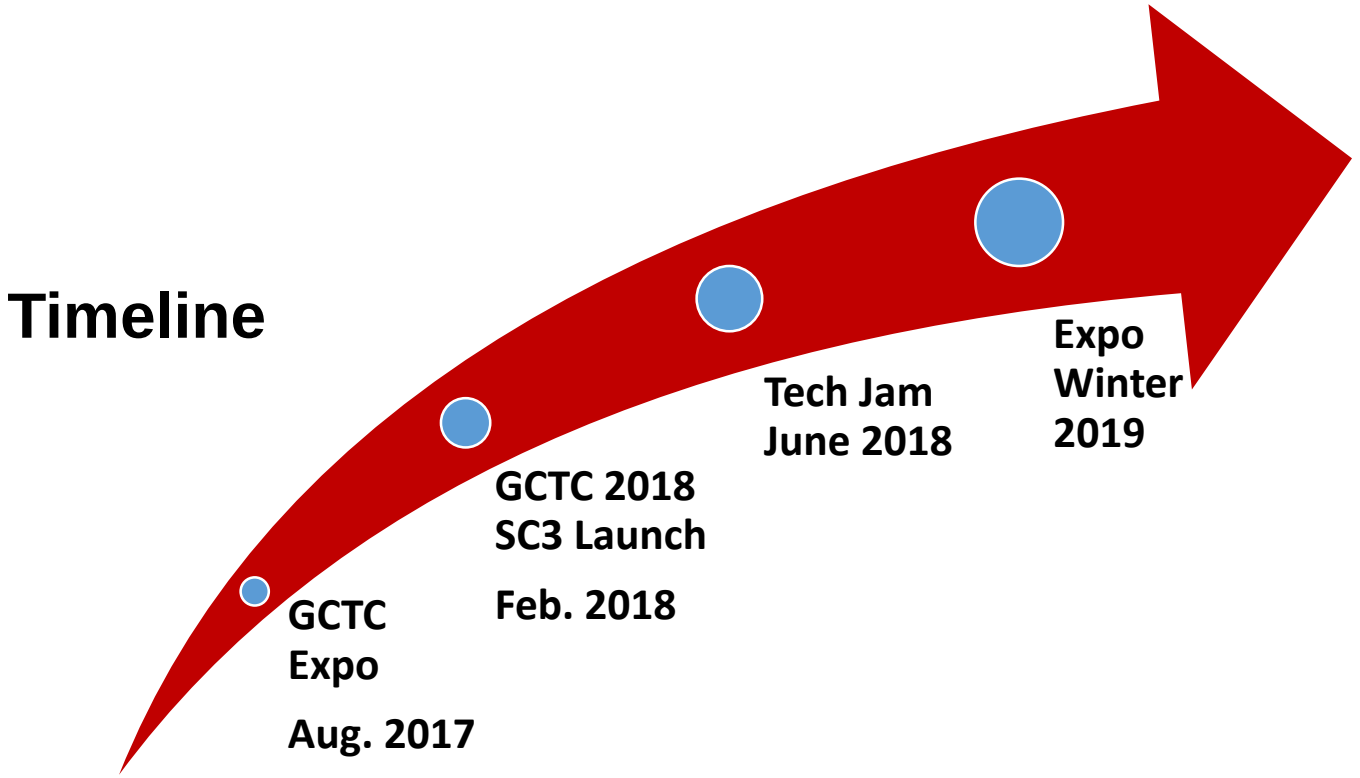
Companies
Universities
National Labs
Int'l Partners

Homeland Security
Cyber Security Division

SC3

DHS S&T and NIST challenge teams of cities and innovators to demonstrate value and return on investment for designed-in trustworthiness for smart city deployments

GCTC – Smart and Secure Cities and Communities Challenge (SC3)



CSD Mission & Strategy

- Aviation Cybersecurity
- Cyber for Critical Infrastructure
- Cyber Physical Systems Security
- Cyber Risk Economics
- Cyber Security for Law Enforcement
- Cybersecurity Outreach
- Cyber.Gov
- Data Privacy Technologies
- Identity Management
- Human Aspects of Cyber Security
- Mobile Security
- Next Gen. Cyber Infrastructure Apex
- Network System Security
- Research Infrastructure
- **Silicon Valley Innovation Program**
- Smart Cities
- Software Assurance
- Transition to Practice

- 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

Silicon Valley Innovation Program

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

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

STREAMLINE

Avg Time to Award: 45 days

LEVERAGE

100:1

$400+M Private Sector

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**

- Topic “calls” released and open for 1 year describe problem set
- 10-page Applications reviewed monthly or quarterly, topic-dependent
- If invited to pitch (15 mins oral), funding decision made within 24 hrs
- Contract awarded on average 30- 45 days – Other Transaction Authority

Topics We're Funding
https://www.dhs.gov/science-and-technology/hsip

Accepting Applications:

Seamless Travel
- High Fidelity Counting & Measuring
- Real-Time, Intelligent Traveler Wayfinding
- Land Border Biometric Facial Recognition

First Responders
- Energy Harvesting Fabrics
- 3D Dynamic Mapping

Aviation Security
- Object Recognition and Adaptive Algorithms

Applications Closed:

Internet of Things Security (Critical Infrastructure, CBP, FPS)

Drones/sUAS Capabilities (CBP)

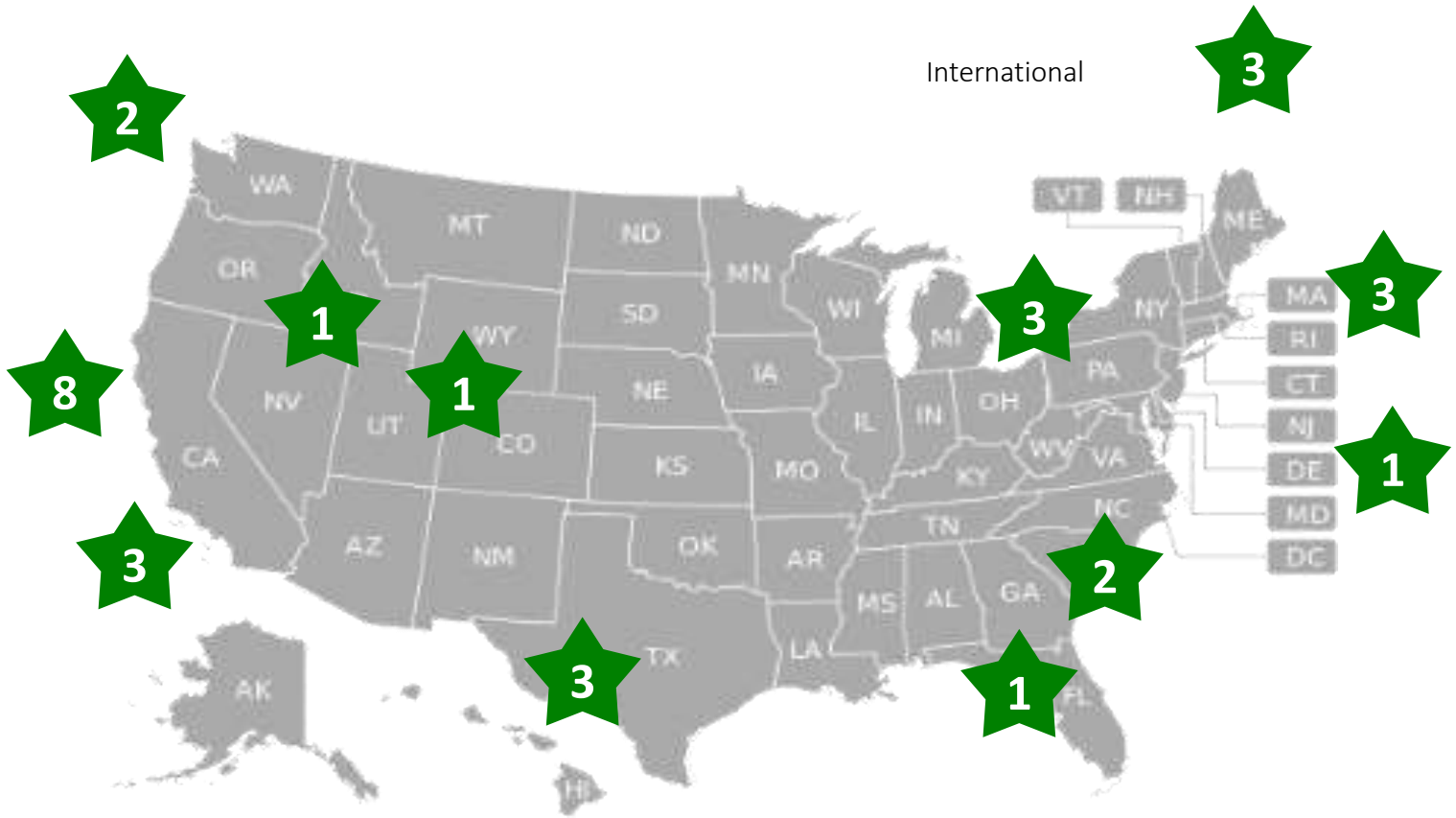
Big Data (CBP)

K9 Wearables (CBP)

Identity & Anti-Spoofing of NPEs

Fintech Cybersecurity (Finance Sector)

Silicon Valley Innovation Program
By the Numbers



45 Days to Contract

13 Funded Topics

$10M Awarded Funding

350 Phase I Applications

31 Startups Funded

57 Phase I Pitches

4 Open Topics

Startups Funded in Each Location

Portfolio Companies

factom

ECHODYNE

skymind

DataRobot

Kiana Analytics

M2Mi
Machine-to-Machine Intelligence Corporation

tamr

omniscience

SHIELD AI

PLANCK

IONIC

PetPace™
Monitoring your pet's health

HaloLights,LLC
|**HaloLights™**

WhiteScope

Bastille

CryptoMove

VERAMINE

StackRox

HEILIG DEFENSE

QED
Secure Solutions

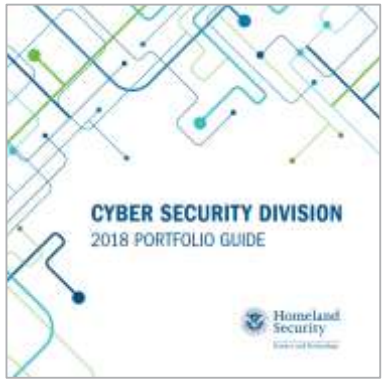
ASYMMETRIC
TECHNOLOGIES

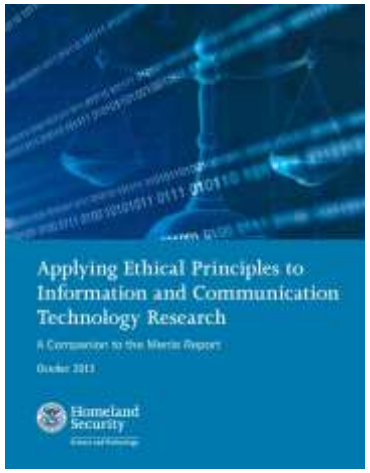
NexiTech

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

CSD Publications: dhs.gov/csd-resources





Douglas Maughan, Ph.D.

Division Director

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

douglas.maughan@dhs.gov

202-254-6145 / 202-360-3170 / 202-836-3278

For more information, visit

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