WELCOME

DHS Science and Technology (S&T)
Cyber Security
Industry Day

Twitter: @dhsscitech

Hashtag: #cyberBAA

Homeland
Security

Industry Day Purpose

- Description of current DHS S&T Cyber Security Division (CSD) Program
- Presentation of Broad Agency Announcement (BAA)
- Presentation of Topics Areas (TTAs) Released to Date
- Industry Day provides opportunities for:
  - (1) understanding S&T CSD’s requirements
  - (2) asking Questions and getting Answers (FAQ)
  - (3) finding partners

Administrative Items

- Questions
  - **ALL** questions must be submitted in writing on 5x8 cards.
  - Please submit Q&A cards to staff at doorways or registration desk as soon as the break begins, or sooner.
  - As many questions as possible will be answered during the Q&A session at the end of the day. Those not answered here will be posted on the BAA FAQ. http://go.usa.gov/kvN5

- Cyber Physical Systems Security (CPSSEC) and Distributed Denial of Service Defense (DDoSD) Industry Days: Thursday, June 26. Registration deadline today, 12:00pm. Onsite registration open. Details at registration desk.

Presentation Agenda

- DHS S&T Cyber Security Division (CSD) Overview
  - Douglas Maughan, DHS S&T HSARPA CSD Director
- BAA Introduction
  - Douglas Maughan, DHS S&T HSARPA CSD Director
- Mobile Technology Security Topic Presentation
  - Luke Berndt, Program Manager, DHS S&T CSD
  - Vincent Sritapan, Technical Lead and Component Coordinator, DHS CISO Office
- BREAK
- Q&A Session

Homeland Security Advanced Research Projects Agency

DHS S&T Cyber Security R&D Programs

Douglas Maughan

Division Director

June 24, 2014

Homeland Security

Science and Technology

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

Presentation Outline

- Threat Space
- U.S. National / Federal Activities
- DHS S&T Activities
- International Participation
- Summary

Cyber Threats and Sources

Nation States

Cyber Criminal Organizations

Terrorists, DTOs, etc.

Insider Threats

Hackers/Hacktivists

- Malware – Malicious software to disrupt computers
- Viruses, worms, …
- Theft of Intellectual Property or Data
- Hactivism – Cyber protests that are socially or politically motivated
- Mobile Devices and Applications and their associated Cyber Attacks
- Social Engineering – Entice users to click on Malicious Links
- Spear Phishing – Deceptive communications (E-Mails, Texts, Tweets)
- Domain Name System (DNS) Attacks
- Router Security – Border Gateway Protocol (BGP) Hijacking
- Denial of Service (DOS) – blocking access to web sites
- Others …..
- **Bottom Line: Easier to be a bad guy and volume of threats is growing**

White House Priorities – FY14+

- Secure Federal Networks
  - Identity/Credential Access Mgmt (ICAM), Cloud Exchange, Fed-RAMP
- Protect Critical Infrastructure
  - Public-Private Cyber Coordination, EO/PPD Initiatives
- Improve Incident Response and Reporting
  - Information Sharing among Federal Centers
  - Capacity Building for State/Local/Tribal/Territorial (SLTTs)
- Engage Internationally
  - Foreign Assistance Capacity Building
  - Build Workforce Capacity to Support International Cyber Engagement
- Shape the Future
  - National Strategy for Trusted Identity in Cyberspace (NSTIC)
  - **National Initiative for Cybersecurity Education (NICE)**
  - **Cybersecurity R&D – EO/PPD R&D Plan, Federal R&D Plan, Transition To Practice, Foundational Research**

Homeland Security
Science and Technology

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities

US Government Departments and Agencies

DOJ/FBI

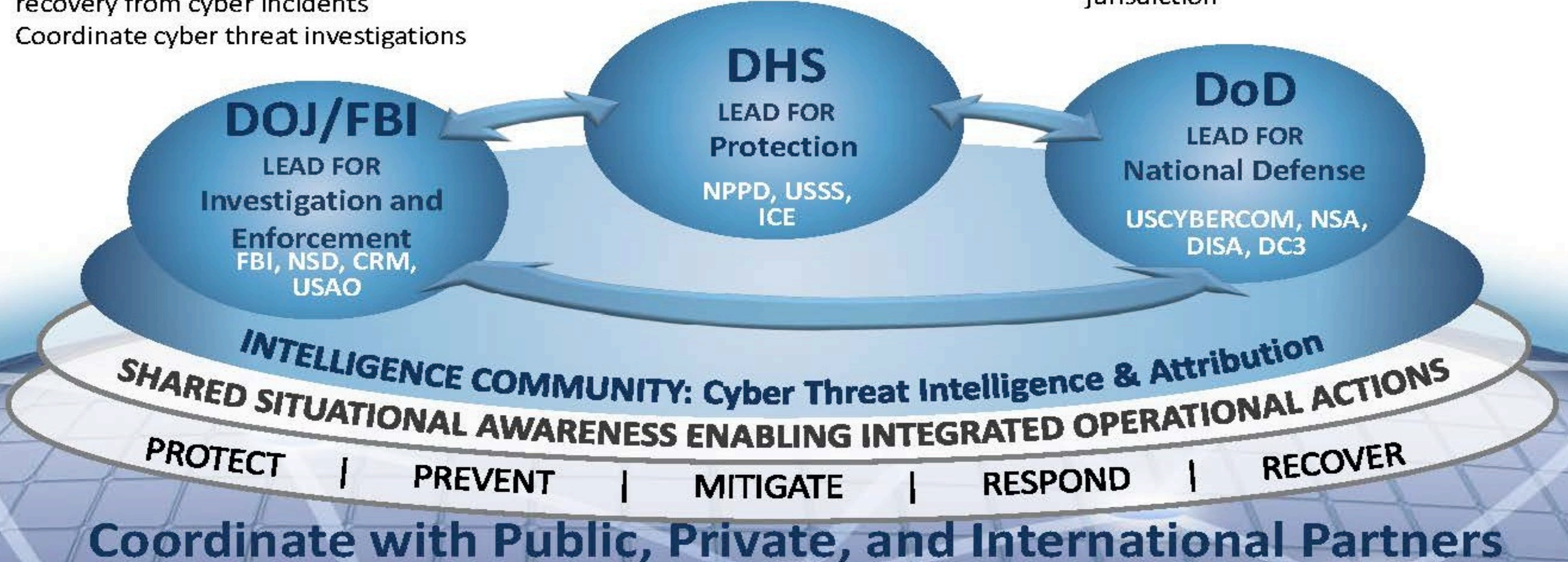
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

DoD

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction


DOJ/FBI
LEAD FOR
Investigation and Enforcement
FBI, NSD, CRM, USAO
DHS
LEAD FOR
Protection
NPPD, USSS, ICE
DoD
LEAD FOR
National Defense
USCYBERCOM, NSA, DISA, DC3
INTELLIGENCE COMMUNITY: Cyber Threat Intelligence & Attribution
SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS
PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

Global Cyberspace

Coordinate with Public, Private, and International Partners

** Note: Nothing in this chart alters existing DOJ, DHS, and DoD roles, responsibilities, or authorities*

UNCLASSIFIED

DHS S&T Mission

Strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise

1) Create new technological capabilities and knowledge products
2) Provide Acquisition Support and Operational Analysis
3) Provide process enhancements and gain efficiencies
4) Evolve US understanding of current and future homeland security risks and opportunities

FOCUS AREAS

- Bio Defense
- Explosives
- Cybersecurity
- First Responders
- Resilient Systems
- Borders / Maritime

CSD Research Requirement Inputs

White House/NSS

- National Strategy 2003
- Comprehensive National Cybersecurity Initiative (CNCI)
- EO 13636/PPD 21
- National CISR R&D Plan (in progress)
- Transition to Practice (TTP)
- Cyber Economic Incentives Research
- National Initiative for Cybersecurity Education (NICE)
- Cybersecurity Framework Support

Departmental Inputs

- QHSR 2009 & 2014
- Blueprint
- NPPD/CS&C/NCCIC
- ICE HSI / IPR
- USSS
- CBP
- USCG
- TSA
- DHS CIO/CISO Councils

Interagency Collaboration

- Cyber Security and Information Assurance (CSIA) IWG
- SCORE – Classified R&D WG
- Cyber-Physical Systems (CPS) SSG
- Big Data SSG
- Cyber Forensics WG

CSD

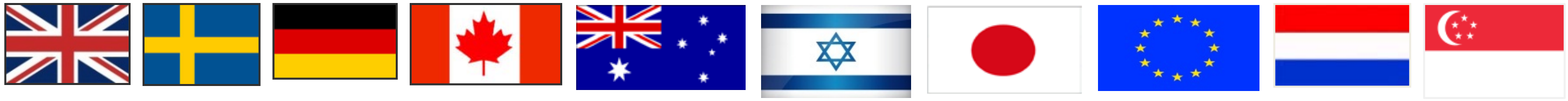
Critical Infrastructure Sectors (Private Sector)

- Energy (Oil & Gas, Electric Power)
- Banking and Finance
- Communications/IT
- Cross-Sector Cyber Security WG

State/Local

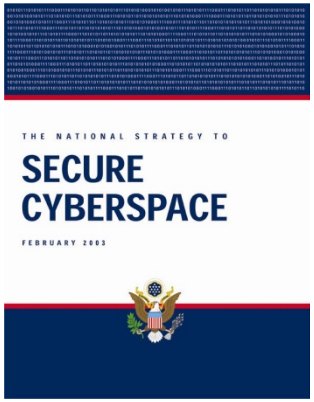
- S&T First Responders Group
- FRAC/TTWG
- SWGDE (FBI)

International Collaborations



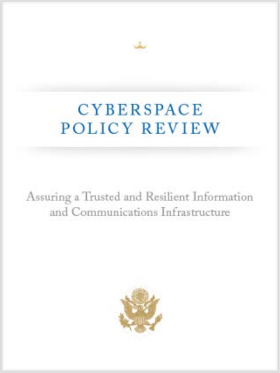
Cybersecurity Requirements Historical Timeline

2003


THE NATIONAL STRATEGY TO
SECURE CYBERSPACE
FEBRUARY 2003

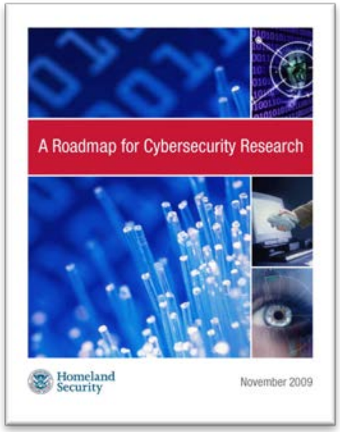
Call for Action
- **Secure Protocols**
  DNSSEC
  Secure Routing
- **DETER security testbed**
- **PREDICT data repository**

2008


CYBERSPACE POLICY REVIEW
Assuring a Trusted and Resilient Information and Communications Infrastructure

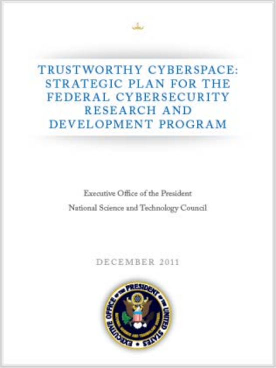
Beginnings of CNCI
- **Call for NICE (Education)**
- **Call for NSTIC (Trusted Identities)**
- **Reinforced need for PREDICT data repository**

2009


A Roadmap for Cybersecurity Research
Homeland Security
November 2009

S&T Produced National R&D Roadmap with community input Source for DHS S&T BAA, SBIR, and other solicitations

2011


TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM
Executive Office of the President
National Science and Technology Council
DECEMBER 2011

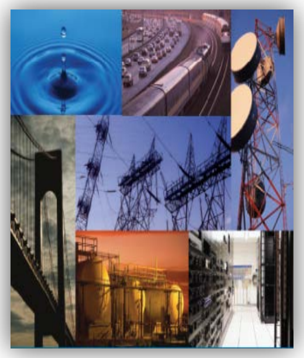
CNCI Tasks 4&9 S&T led via co-chair of CSIA IWG Significant inter-agency activities initiated by WH/NSS/OSTP

2012

Blueprint for a Secure Cyber Future
The Cybersecurity Strategy for the Homeland Security Enterprise
November 2011
Homeland Security

Implementation plan to accomplish goals of DHS QHSR 24 high priority capabilities needed NPPD-led, S&T involved

2013



EO 13636: Improving Critical Infrastructure Cybersecurity

PPD 21: Critical Infrastructure Security and Resilience

2013 HSARPA R&D Strategy – 10 Themes, 43 Priority areas, 320+ Focus areas
Inputs from WH/NSS, DOE, Treasury, GSA, DHS CISO, NPPD/CS&C, USSS/ICE/CBP

CSD Mission & Strategy

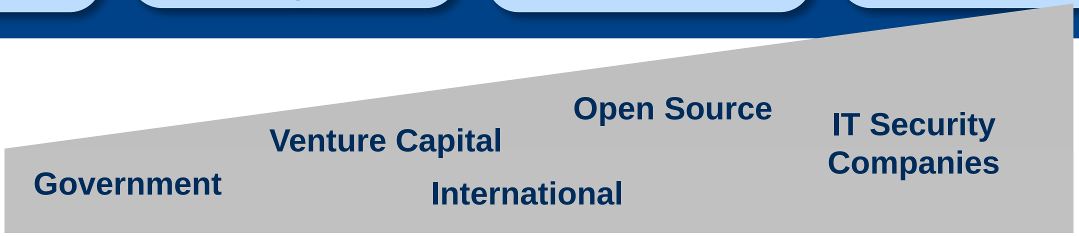
REQUIREMENTS

CSD MISSION

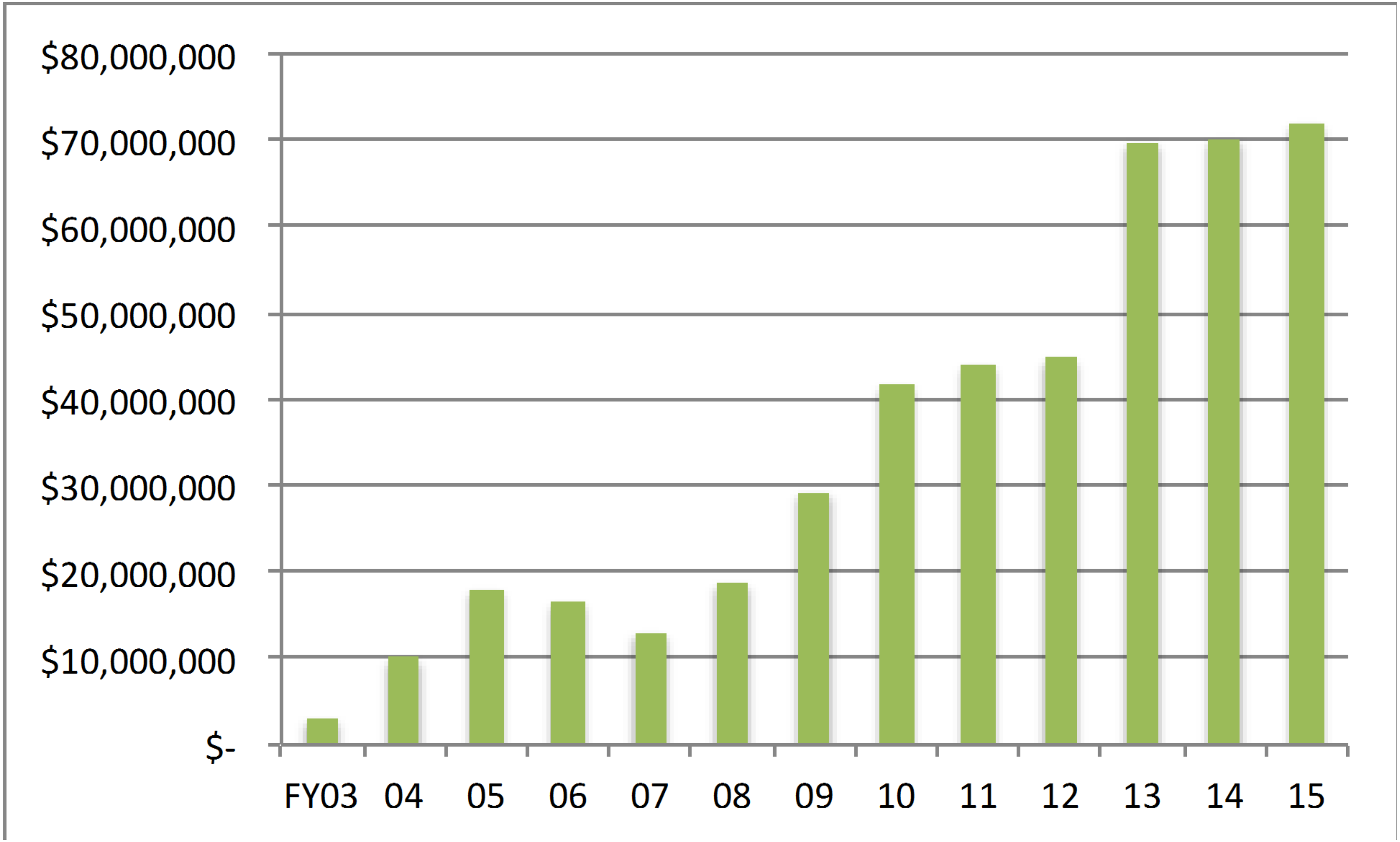
- **Develop and deliver new technologies, tools and techniques** to defend and secure current and future systems and networks
- Conduct and support **technology transition** efforts
- Provide **R&D leadership and coordination** within the government, academia, private sector and international cybersecurity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

CSD STRATEGY

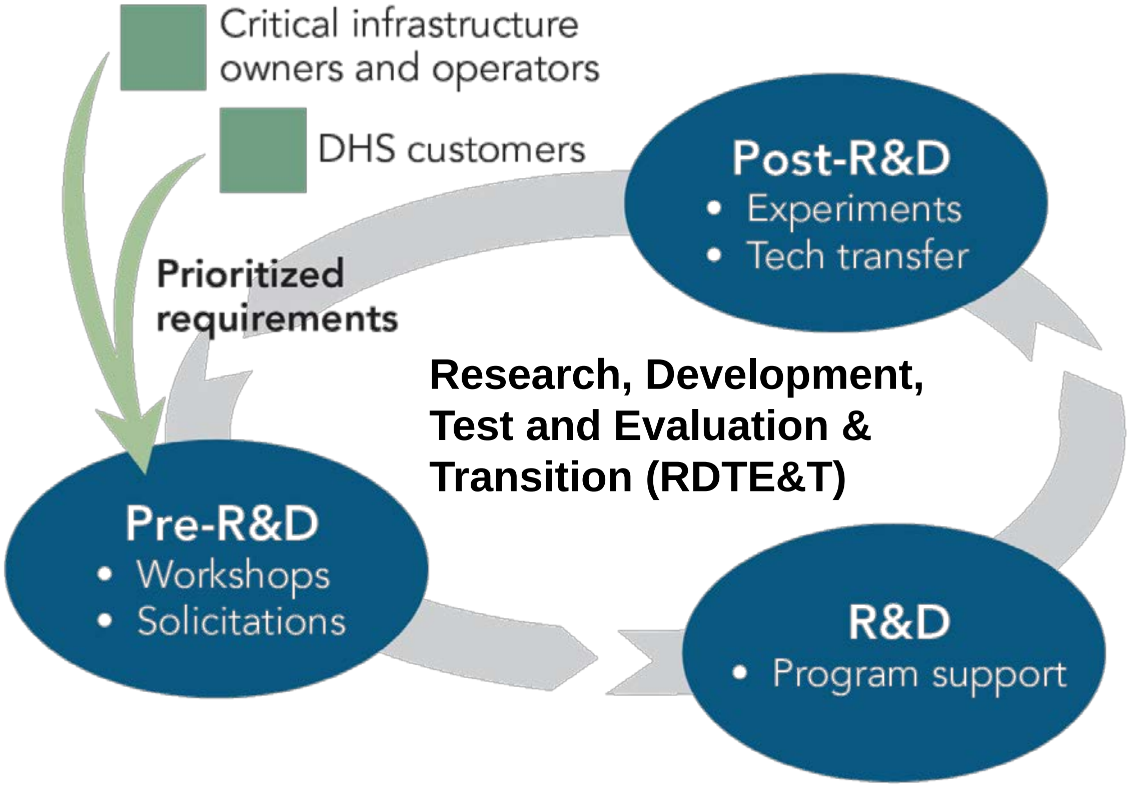
- Trustworthy Cyber Infrastructure
- Cybersecurity Research Infrastructure
- Network & System Security and Investigations
- Cyber Physical Systems
- Transition and Outreach



Cyber Security Budget Overview



CSD R&D Execution Model



🟩 Critical infrastructure owners and operators

🟩 DHS customers

Prioritized requirements

Post-R&D
- Experiments
- Tech transfer

Pre-R&D
- Workshops
- Solicitations

R&D
- Program support

Research, Development, Test and Evaluation & Transition (RDTE&T)

"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

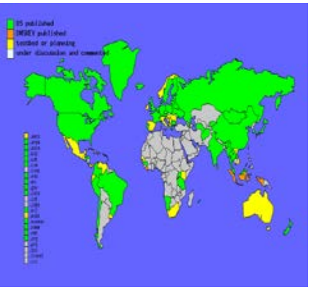
Successes

Over 30 products transitioned since 2004, including:

- 2004 – BAA 04-17
  - 5 commercial products
  - 2 Open Source products
- 2005 – BAA 05-10 (RTAP)
  - 1 commercial product
  - 1 GOTS product
  - 1 Open Source product
- 2007 – BAA 07-09
  - 2 commercial products
- 2011 – BAA 11-02 (more to come)
  - 1 Open Source product
  - 1 Research Infrastructure
- Law Enforcement Support
  - 2 commercial products
  - 1 Open Source product
  - Multiple Knowledge products
- Identity Management
  - 1 Open Source standard and GOTS solution
- SBIRs
  - 8 commercial products
  - 1 Open Source product

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

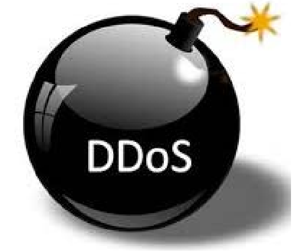


Secure Protocols

- 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)

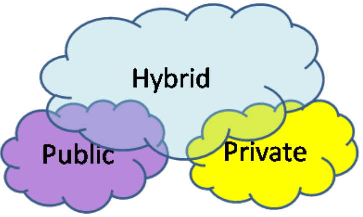
- Policy-based technologies to shift the advantage to the defender
- Measurement/analysis tools to test success of BCP38 deployments
- Engaging with major finance sector companies and supporting ISPs

Homeland Security

Science and Technology

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

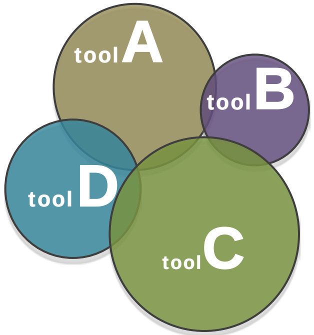
- Develop new approaches to mobile device security (user identity/authentication, device management, App security and management, and secure data) for government purposes
- Working with DHS CISO and across several components

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

CORE INSIGHT ENTERPRISE

SECURITY TESTING EXECUTIVE REPORT

TESTING SUMMARY

EXPOSURE DISTRIBUTION

COMPROMISED ASSETS

EXPOSURE OVER TIME

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

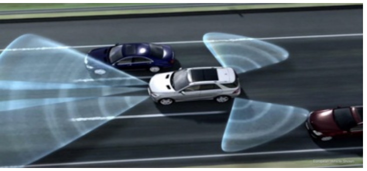
Investigation Capabilities for Law Enforcement

- 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

Homeland Security
Science and Technology

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) – *RSD collaboration*

- 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

TCIPG

Trustworthy Computing Infrastructure for the Power Grid (TCIPG)

- Improve the security of next-generation power grid infrastructure, making the underlying infrastructure more secure, reliable and safe
- 4 University consortium – UIUC, WSU, UC-Davis, Dartmouth
- Private sector advisory board provides reqmts and transition path
- Partnership with DOE ($12M); Planning joint FY15 recompete

LOGIIC

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

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

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 (PREDICT)

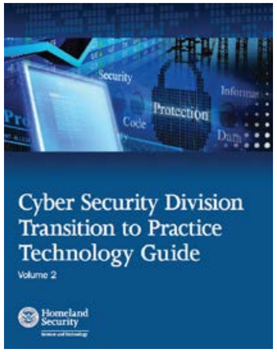
- Repository of over 700TB of network data for use by community
- More than 250 users (academia, industry, gov't – NSA SBIR)
- Leading activities on ICT Research Ethics (e.g., Menlo Report)
- Opening up to international partners (JP, CA, AU, UK, IL, EU)

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; 500+ assessments/week; 8 platforms; 5 SwA tools

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



Cyber Security Division
Transition to Practice
Technology Guide
Volume 2

Homeland Security

Transition To Practice (TTP)

- White House initiated program; CSD budget plus-up in FY12
- Working with DOE and DOD labs, FFRDCs, UARCs, NSF, SBIRs
- Developing relationships in the Energy and Finance Sectors
- Multiple pilots in progress; Two commercial licensing deals done

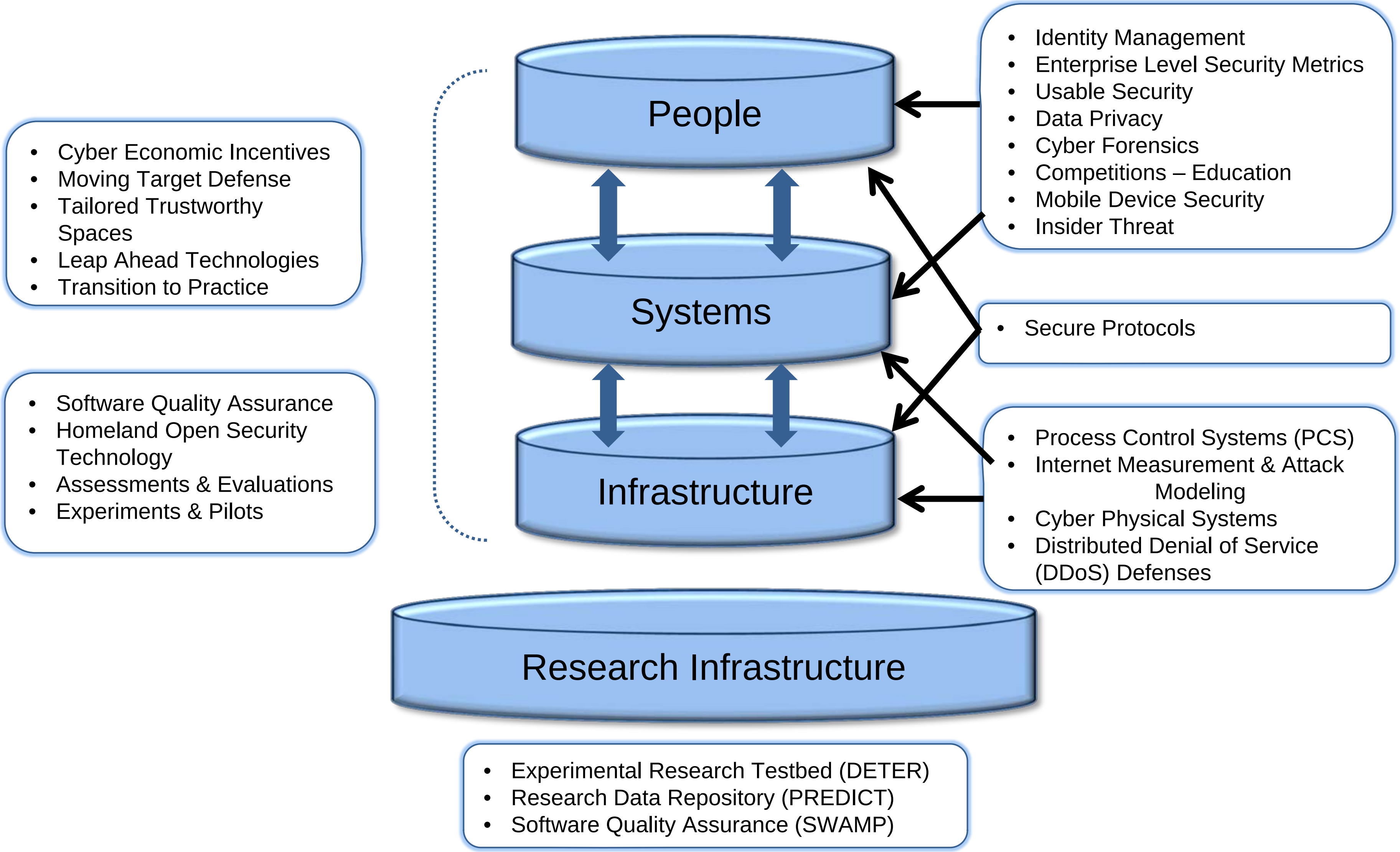
Cybersecurity Competitions

- Provide a controlled, competitive environment to assess a student's understanding and operational competency
- CSD-funded technologies included for test and evaluation
- 180+ schools and 1500+ college students participated in 2014
- 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)
- National Academic Consortiums – FY14 solicitation thru NIST

CSD Projects / Relationships



- Cyber Economic Incentives
- Moving Target Defense
- Tailored Trustworthy Spaces
- Leap Ahead Technologies
- Transition to Practice

- Software Quality Assurance
- Homeland Open Security Technology
- Assessments & Evaluations
- Experiments & Pilots

People

Systems

Infrastructure

- Identity Management
- Enterprise Level Security Metrics
- Usable Security
- Data Privacy
- Cyber Forensics
- Competitions – Education
- Mobile Device Security
- Insider Threat

- Secure Protocols

- Process Control Systems (PCS)
- Internet Measurement & Attack Modeling
- Cyber Physical Systems
- Distributed Denial of Service (DDoS) Defenses

Research Infrastructure

- Experimental Research Testbed (DETER)
- Research Data Repository (PREDICT)
- Software Quality Assurance (SWAMP)

Homeland Security
Science and Technology

S&T International Engagements

- **International Bilateral Agreements**
  - **Government-to-government cooperative activities for 13 bilateral Agreements**

- **Canada (2004)**
- **Australia (2004)**
- **United Kingdom (2005)**
- **Singapore (2007)**
- **Sweden (2007)**
- **Mexico (2008)**
- **Israel (2008)**
- **France (2008)**
- **Germany (2009)**
- **New Zealand (2010)**
- **European Commission (2010)**
- **Spain (2011)**
- **Netherlands (2013)**

European Commission
Sweden
The Netherlands
Canada
United Kingdom
Germany
Spain
France
DHS
Israel
Mexico
Singapore
Australia
New Zealand

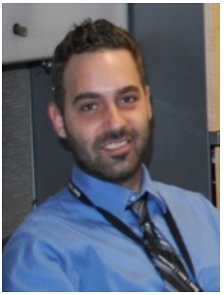
COUNTRY	PROJECTS	MONEY IN	JOINT	MONEY OUT
Australia	3	$300K	$400K	
Canada	11	$1.8M		
Germany	1		$300K	
Israel	2		$100K	
Netherlands	7	$450K	$1.2M	$150K
Sweden	4	$650K		
United Kingdom	3	$1.0M	$400K	$200K
European Union	1			
Japan	1			

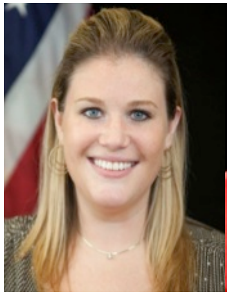
Over $6M of International co-funding

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
  - Particular challenges include scope/complexity of the different areas of the problem, and the balance of near 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 the best ideas and solutions to real-world problems

Luke **Berndt**


Matt **Billone**


Amelia **Brown**

Kyshina **Chandler**

Ann **Cox**

Shane **Cullen**

John **Drake**

Nicole **Fisher**

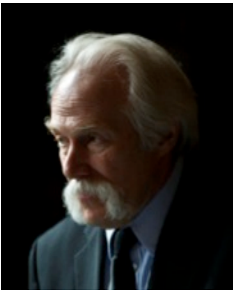
Tammi **Fisher**

Brendon **Gibson**

Kevin **Greene**

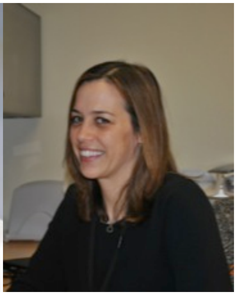
Karyn **Higa-Smith**

Melissa **Ho**

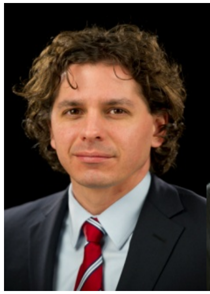

Joe **Kielman**

Megan **Mahle**

Dan **Massey**


Jennifer **Mekis**

Derrick **Nelson**


Mike **Pozmantier**

Mike **Reagan**

Ed **Rhyne**

Emily **Saulsgiver**

Yolanda **Saunders**

Shelby **Smith**

Scott **Tousley**

Greg **Wigton**

Douglas Maughan, Ph.D.

Division Director

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

douglas.maughan@dhs.gov

202-254-6145

For more information, visit

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

Homeland Security

Science and Technology