Homeland Security Advanced Research Projects Agency

An Update from Washington: What's Happening in the World of Cyber Security and Critical Infrastructure

Douglas Maughan

Division Director

November 12, 2014

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

Homeland Security

Science and Technology

Presentation Outline

- Threat Space
- U.S. National / Federal / Department Activities
- DHS S&T Activities
  - S&T Visionary Goals
  - Cyber Security R&D Program
- International Participation
- Solicitations
  - FY14 BAA
    - Cyber Physical Systems Security (CPSSEC)
    - Distributed Denial of Service Defenses (DDOSD)
    - Mobile Security Technology
    - Data Privacy Technologies
- 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**

Homeland Security
Science and Technology

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**

Executive Order (EO) on Improving Critical Infrastructure Cybersecurity/ Policy Presidential Directive (PPD) on Critical Infrastructure Security and Resilience

Credit: White House / Pete Souza

"America must also face the rapidly growing threat from cyber attacks… That's why, earlier today, I signed a new executive order that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy."

President Barack Obama,
2013 State of the Union

Executive Order 13636: Improving Critical Infrastructure Cybersecurity directs the Executive Branch to:

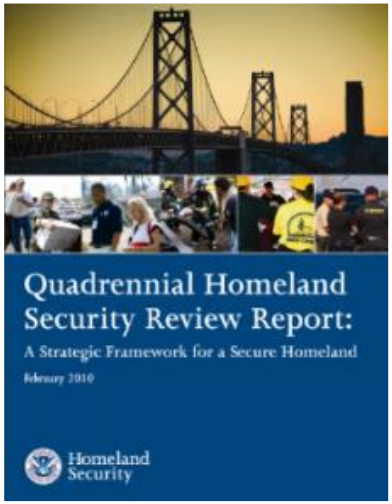
- Develop a technology-neutral voluntary cybersecurity framework
- Promote/incentivize adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore existing regulation to promote cyber security

Presidential Policy Directive-21: Critical Infrastructure

- Security and Resilience replaces Homeland Security Presidential Directive-7 and directs 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 cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Homeland Security

DHS Requirements - QHSR



February 2010

- **Mission 4: Safeguarding and Securing Cyberspace**
- **Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment. Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure.**
  - Understand and prioritize cyber threats
  - Manage risks to cyberspace
  - Prevent cyber crime and other malicious uses of cyberspace
  - Develop a robust public-private cyber incident response capability
- **Goal 4.2 Promote Cybersecurity Knowledge and Innovation. Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.**
  - Enhance public awareness
  - Foster a dynamic workforce
  - <u>Invest in innovative technologies, techniques, and procedures</u>

Homeland Security
Science and Technology

Homeland Security
Science and Technology

2014 QHSR

MISSION 4: SAFEGUARD AND SECURE CYBERSPACE

Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure

- Enhance the exchange of information and intelligence on risks to critical infrastructure and develop real-time situational awareness capabilities that ensure machine and human interpretation and visualization;
- Partner with critical infrastructure owners and operators to ensure delivery of essential services and functions;
- Identify and understand interdependencies and cascading impacts among critical infrastructure systems ;
- Collaborate with agencies and the private sector to identify and develop effective cybersecurity policies and best practices; and
- Reduce vulnerabilities and promote resilient critical infrastructure design.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

- Coordinate government purchasing of cyber technology to enhance cost-effectiveness;
- Equip civilian government networks with innovative cybersecurity tools and protections; and
- Ensure government-wide policy and standards are consistently and effectively implemented and measured.

Goal 4.3: Advance Law Enforcement, Incident Response, and Reporting Capabilities

- Respond to and assist in the recovery from cyber incidents; and
- Deter, disrupt, and investigate cybercrime.

Goal 4.4: 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.

2014 CYBER SECURITY DIVISION R&D SHOWCASE AND TECHNICAL WORKSHOP

Homeland Security
Science and Technology

R&D SHOWCASE:

The R&D Showcase will feature 11 innovative technologies selected from the Cyber Security Division (CSD) portfolio that address today's complex cybersecurity challenges and have the potential for transition into the marketplace. Technology presentations will showcase results from Modeling of Internet Attacks, Cybersecurity Competitions, Identity Management, Cybersecurity Forensics, Software Quality Assurance, Transition to Practice, Process Control Systems, Leap Ahead Technologies, Research Data Repositories, Experimental Research Testbeds, and Cyber Economic Incentives. The showcase will also feature a technology demonstration and poster session, giving participants the opportunity to learn about the division's portfolio.

TECHNICAL WORKSHOP:

The two-day technical workshop features CSD Principal Investigators (PIs) presenting their research and technologies to researchers and cyber security leadership from the government, international partners, private sector and academia. The workshop will allow for additional collaboration and knowledge sharing, improvement of existing deployed technologies and transition of innovative research to safeguard cyberspace.

Science and Technology

December 16-18, 2014

R&D SHOWCASE:
December 16, 2014

TECHNICAL WORKSHOP:
December 17 & 18, 2014

Mayflower Renaissance Hotel

1127 Connecticut Ave NW
Washington, DC

WHO SHOULD ATTEND

R&D SHOWCASE:

Registration for the R&D Showcase is open to public and private sector cybersecurity professionals, Congress and the media.

TECHNICAL WORKSHOP:

Registration for the Technical Workshop is open to invited DHS S&T cybersecurity PIs, customers, and international partners.

REGISTRATION

To register, go to:
http://events.SignUp4.com/2014RDShowcase

Registration is complimentary.

The Future at DHS S&T - 1

S&T'S VISIONARY GOALS

- **Screening at Speed: Security that Matches the Pace of Life**
  - Noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Unobtrusive screening of people, baggage or cargo will enable the seamless detection of threats while respecting privacy, with minimal impact to the pace of travel and speed of commerce.
- **A Trusted Cyber Future: Protecting Privacy, Commerce and Community**
  - In a future of increasing cyber connections, underlying digital infrastructure will be self-detecting, self-protecting and self-healing. Users will trust that information is protected, illegal use is deterred, and privacy is not compromised. Security will operate seamlessly in the background.

The Future at DHS S&T - 2

S&T'S VISIONARY GOALS

- **Enable the Decision Maker: Actionable Information at the Speed of Thought**
  - Predictive analytics, risk analysis and modeling-and-simulation systems will enable critical and proactive decisions to be made based on the most relevant information, transforming data into actionable information. Even in the face of uncertain environments involving chemical, biological, radiological or nuclear incidents, accurate, credible and context-based information will empower the aware decision maker to take instant actions to improve critical outcomes.
- **Responder of the Future: Protected, Connected, and Fully Aware**
  - The responder of the future is threat-adaptive and cross-functional. Armed with comprehensive physical protection, interoperable tools and networked threat detection and mitigation capabilities, responders of the future will be better able to serve their communities.

The Future at DHS S&T - 3

S&T'S VISIONARY GOALS

- **Resilient Communities: Disaster-Proofing Society**
  - Critical infrastructure of the future will be designed, built and maintained to withstand naturally-occurring and man-made disasters. Decision makers will know when disaster is coming, anticipate the effects, and use already-in-place or rapidly-deployed countermeasures to shield communities from negative consequences. Resilient communities struck by disasters will not only bounce back, but bounce forward.

Homeland Security
Science and Technology

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

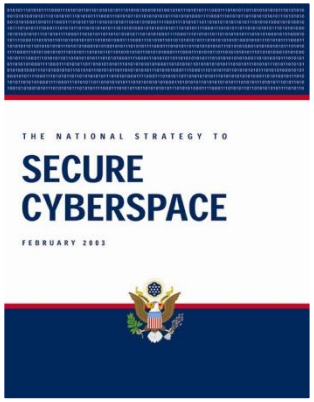
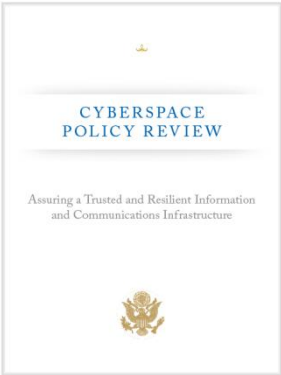
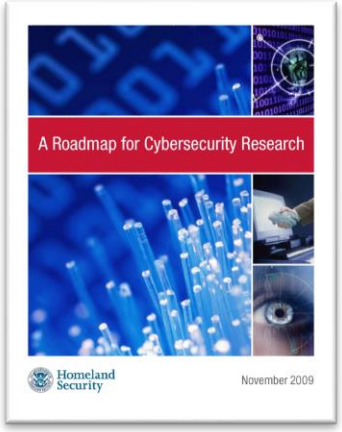
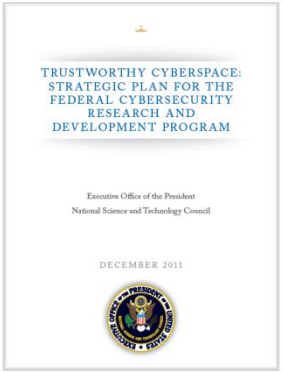
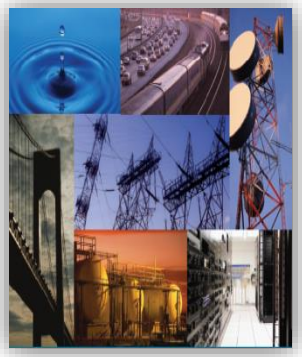
CSD

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

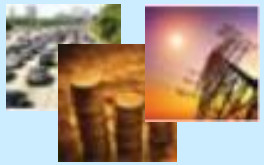
2003	2008	2009	2011	2012	2013
					
Call for Action - **Secure Protocols** DNSSEC Secure Routing - **DETER security testbed** - **PREDICT data repository**	**Beginnings of CNCI** - **Call for NICE (Education)** - **Call for NSTIC (Trusted Identities)** - **Reinforced need for PREDICT data repository**	**S&T Produced National R&D Roadmap with community input Source for DHS S&T BAA, SBIR, and other solicitations**	**CNCI Tasks 4&9 S&T led via co-chair of CSIA IWG Significant inter-agency activities initiated by WH/NSS/OSTP**	**Implementation plan to accomplish goals of DHS QHSR 24 high priority capabilities needed NPPD-led, S&T involved**	**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

Homeland Security
Science and Technology

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

Stakeholders

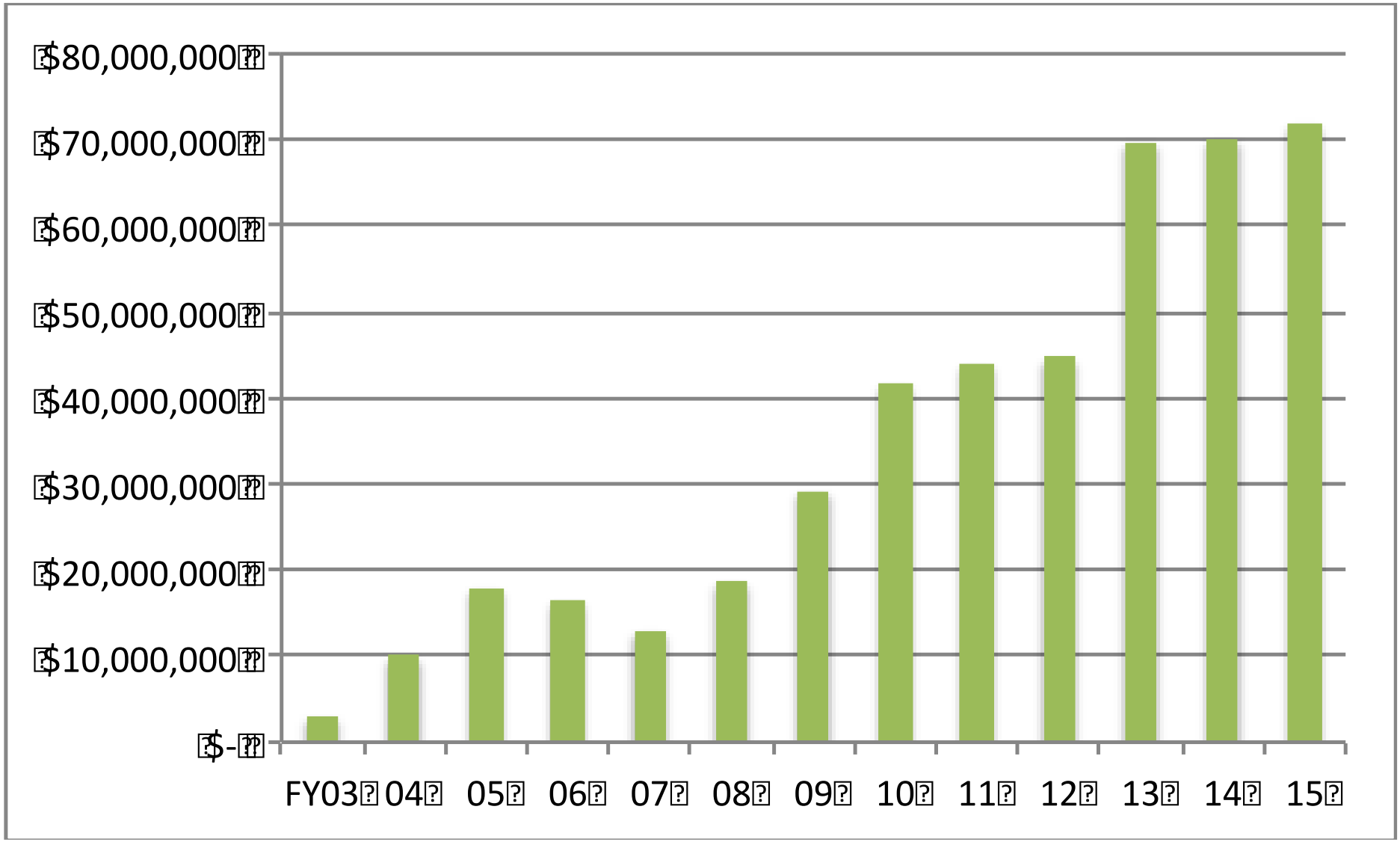
Government
Venture Capital
International
IT Security Companies
Open Source

Outreach Methods (Sampling)

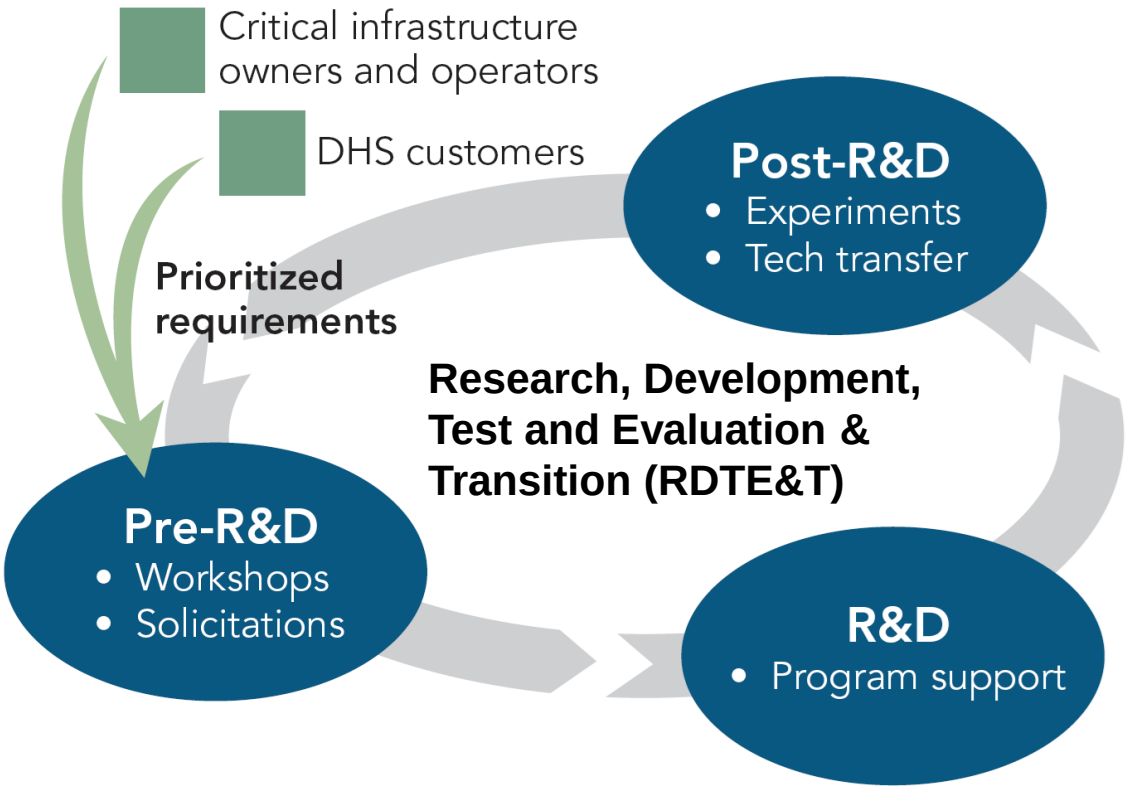
Technology Demonstrations
Speaking Engagements
Program Reviews
Social Media
Media Outreach

Homeland Security
Science and Technology

Cyber Security Budget Overview



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

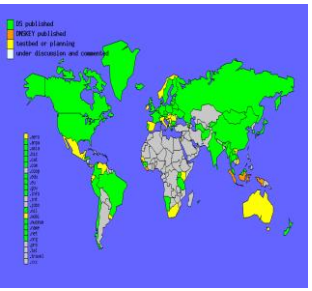
Successes

Over 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

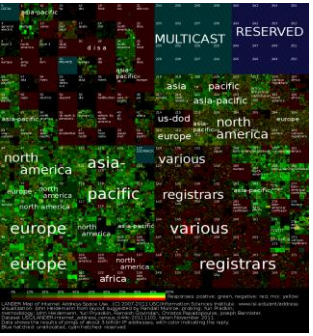
Trustworthy Cyber Infrastructure

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)

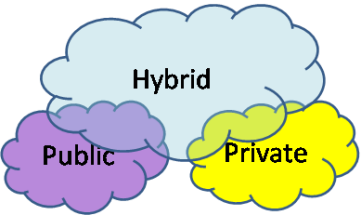
- Create more complete view of the geographical and topological mapping of networks and systems
- Improve global peering, geo-location, and router level maps to assist automated solutions for attack prevention, detection, response
- Support cross-org, situational understanding at multiple time scales

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

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

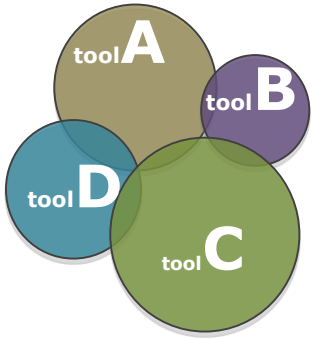
- Develop new approaches to mobile device security (user identity/authentication, device management, App security and management, and secure data) for government purposes
- Working with DHS CISO and across several components

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

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-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

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)

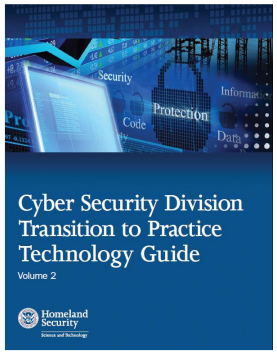
- Repository of over 700TB of network data for use by community
- More than 250 users (academia, industry, gov't – NSA SBIR)
- Leading activities on ICT Research Ethics (e.g., Menlo Report)
- Opening up to international partners (JP, CA, AU, UK, IL, EU)

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; 9 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



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

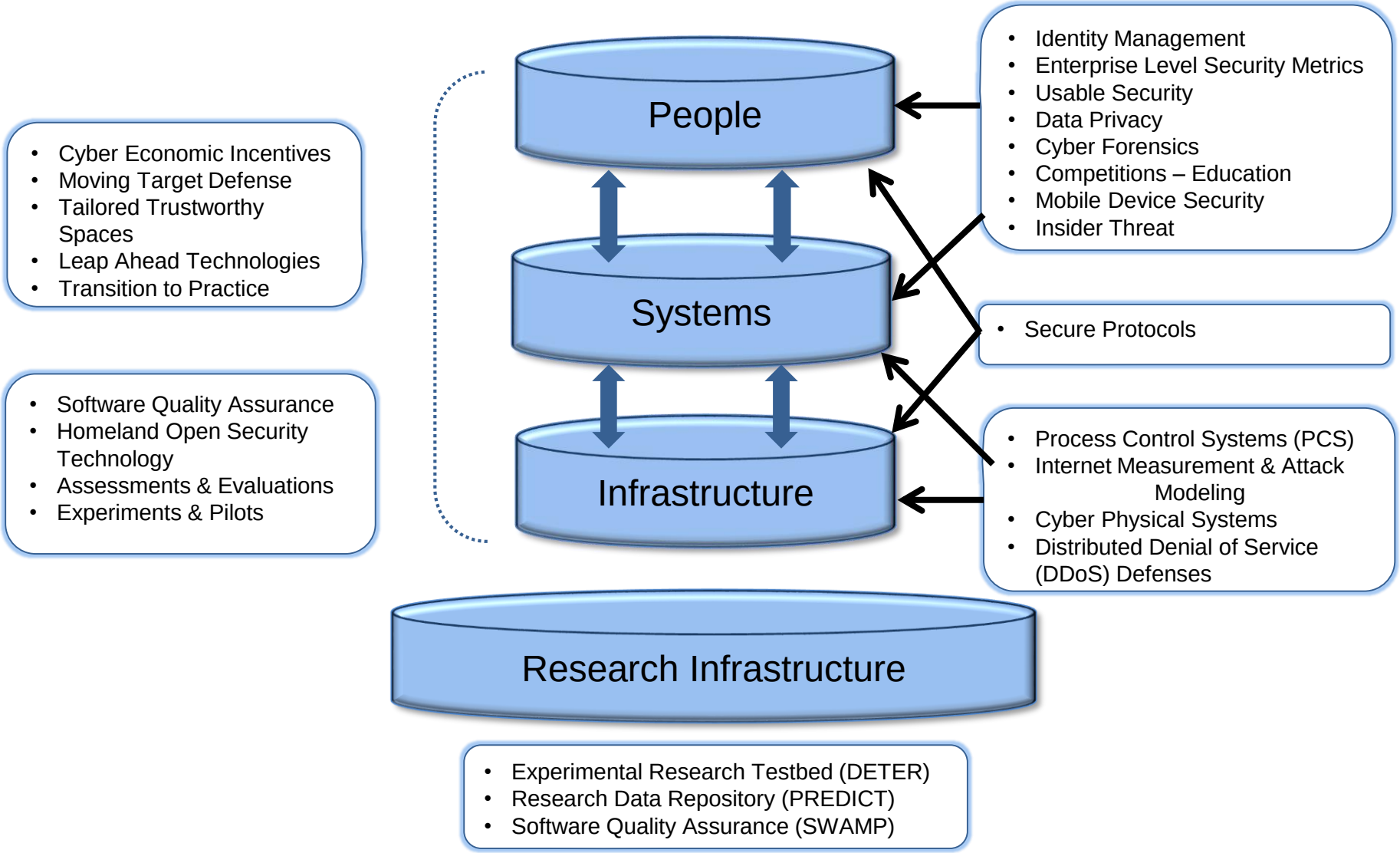
Cybersecurity Competitions

- 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)
- Regional Alliances for Cyber Education (RACE) – FY15 solicit. thru NIST

CSD Projects / Relationships



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)**

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
New Zealand	1			
Japan	1			

Over $6M of International co-funding

2014 Broad Agency Announcement

- Anticipated Schedule
  - 23 Apr: BAA released incl. to participating countries
    - $95M over 5 year period
  - https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-14-R-B0005/listing.html
  - S&T BAA Website: https://baa2.st.dhs.gov
  - 1 June+: Publish BAA Topic Calls
    - Open to all respondents – foreign and domestic
  - June 2014 – March 2015: BAA White Paper and Proposal Review process and Contracting Activities

International Collaborations

2014 BAA – Topics

- Data Privacy: http://go.usa.gov/8JZ9
  - TTA #1 - Privacy Policy Compliance Tools
  - TTA #2 - Privacy-Preserving Federated Search
  - TTA #3 - Mobile Computing Privacy
- Mobile Tech Sec: http://go.usa.gov/8JBY
  - TTA #1 - Mobile Device Instrumentation
  - TTA #2 - Transactional Security Methods
  - TTA #3 - Mobile Security Mgmt Tools
  - TTA #4 - Protecting Mobile Device Layers
- CPSSEC: http://go.usa.gov/8JBQ
  - TTA #1 - Security Models and Interactions
  - TTA #2 - Secure System Design and Implementation
  - TTA #3 - Experiments and Pilots
- DDoSD: http://go.usa.gov/8JBB
  - TTA #1 - Measurement & Analysis to Promote Best Current Practices (BCP 38, SAC004)
  - TTA #2 - Tools for Communication and Collaboration
  - TTA #3 - Novel DDoS Attack Mitigation and Defense Techniques

Homeland Security
Science and Technology

CSD New Programs / Ideas

- Security for Cloud-Based Systems
- Mobile Wireless Investigations
- Application Security Threat Attack Modeling (ASTAM)
- Static Tool Analysis Modernization Project (STAMP)
- Network Reputation and Risk Analysis
- Data Analytics Methods for Cyber Security
- Cyber Security Education
- Designed-In Security
- Finance Sector Cybersecurity
- DNSSEC Applications
- Data Provenance for Cybersecurity
- Cyber Economic Incentives – based on EO/PPD
- Human-centered cybersecurity
- Internet Situational Awareness – based on EO/PPD
- Cybersecurity Metrics

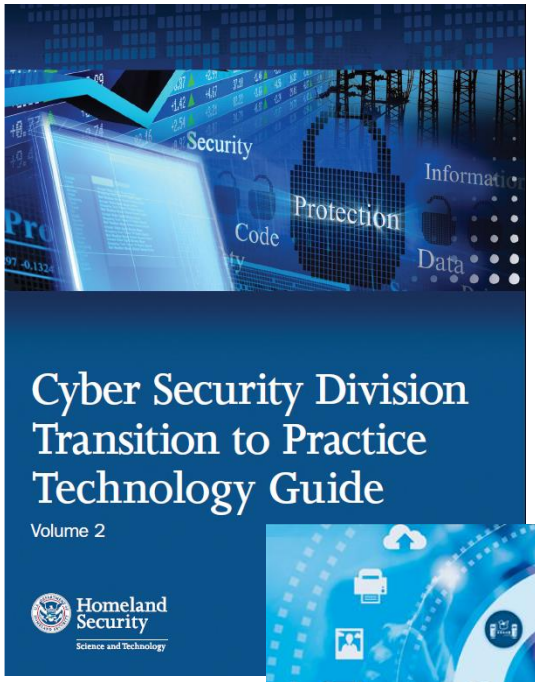
Homeland Security
Science and Technology

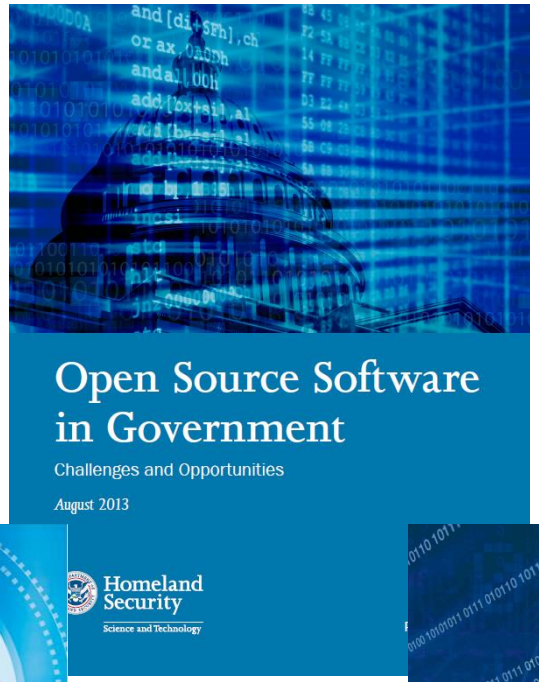
Summary / Conclusions

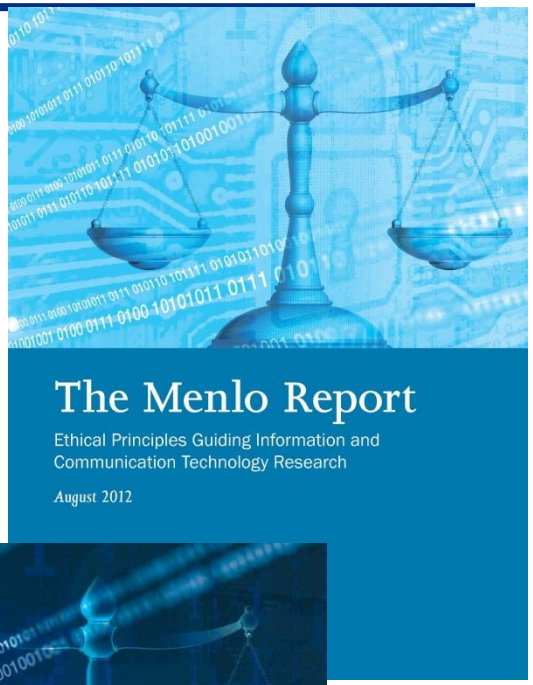
- Cybersecurity research is a key area of innovation to support our global economic and national security futures
- CSD continues with an aggressive cyber security research agenda to solve the cyber security problems of our current and future infrastructure and systems
  - Particular challenges include 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

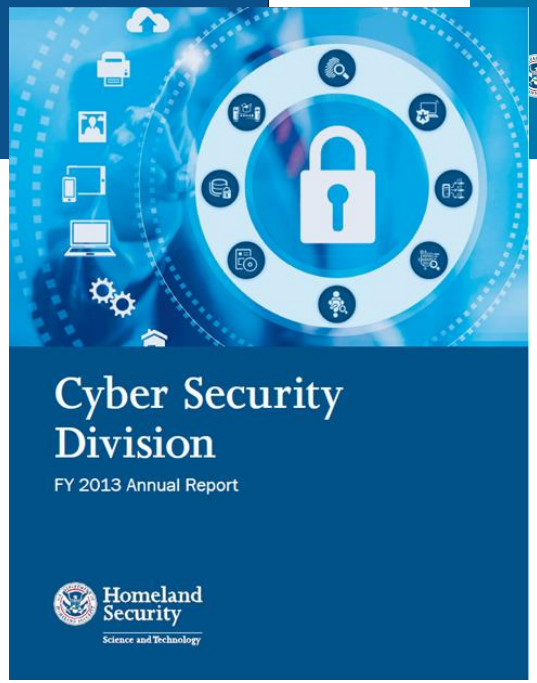
Homeland Security
Science and Technology

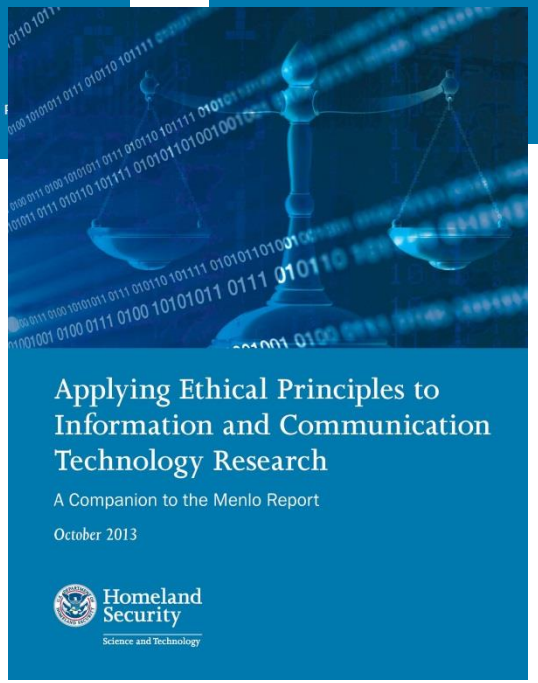
Recent CSD Publications











2014 CYBER SECURITY DIVISION R&D SHOWCASE AND TECHNICAL WORKSHOP

Homeland Security
Science and Technology

R&D SHOWCASE:

The R&D Showcase will feature 11 innovative technologies selected from the Cyber Security Division (CSD) portfolio that address today's complex cybersecurity challenges and have the potential for transition into the marketplace. Technology presentations will showcase results from Modeling of Internet Attacks, Cybersecurity Competitions, Identity Management, Cybersecurity Forensics, Software Quality Assurance, Transition to Practice, Process Control Systems, Leap Ahead Technologies, Research Data Repositories, Experimental Research Testbeds, and Cyber Economic Incentives. The showcase will also feature a technology demonstration and poster session, giving participants the opportunity to learn about the division's portfolio.

TECHNICAL WORKSHOP:

The two-day technical workshop features CSD Principal Investigators (PIs) presenting their research and technologies to researchers and cyber security leadership from the government, international partners, private sector and academia. The workshop will allow for additional collaboration and knowledge sharing, improvement of existing deployed technologies and transition of innovative research to safeguard cyberspace.

December 16-18, 2014

R&D SHOWCASE:
December 16, 2014

TECHNICAL WORKSHOP:
December 17 & 18, 2014

Mayflower Renaissance Hotel

1127 Connecticut Ave NW
Washington, DC

WHO SHOULD ATTEND

R&D SHOWCASE:

Registration for the R&D Showcase is open to public and private sector cybersecurity professionals, Congress and the media.

TECHNICAL WORKSHOP:

Registration for the Technical Workshop is open to invited DHS S&T cybersecurity PIs, customers, and international partners.

REGISTRATION

To register, go to:
http://events.SignUp4.com/2014RDShowcase

Registration is complimentary.

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

For more information, visit

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

Homeland Security

Science and Technology