

Homeland Security Advanced Research Projects Agency

The Bigger Picture: S&T's Role in Cyber Security

August 15, 2013

TTP - Finance Sector

Douglas Maughan

Division Director



Homeland Security

Science and Technology



<http://www.cyber.st.dhs.gov>

Environment: Greater Use of Technology, More Threats, Less Resources



MORE THREATS

RESOURCES
LESS



Comprehensive National Cybersecurity Initiative (CNCI)



Establish a front line of defense

Focus Area 1

Rec... of e

Operational – NPPD and Inter-agency (S&T supporting NPPD)

S&T – part of SSG

Coordinate and Redirect Efforts

Resolve to secure cyberspace / set conditions for long-term success

Focus Area 2

Connect Current Centers to Enhance Situational Awareness

Classified – Intel Community/Inter-agency

Develop Gov't-wide Counterintelligence S&T CSD not involved

Improve Security of the Classified Networks

NICE – S&T involved

Expand Education

Shape future environment / secure U.S. advantage / address new threats

Focus Area 3

Define and Develop Enduring Technologies, Strategies & Programs

S&T – Add'l Funds Rec'd

Define and Develop Enduring Deterrence Strategies & Programs

Inter-agency Programs

S&T CSD not involved

Manage Global Supply Chain Risk

NIPP -S&T involved

Cyber Security in Critical Infrastructure



U.S. Federal Cybersecurity Operations Team National Roles and Responsibilities

DOJ/FBI

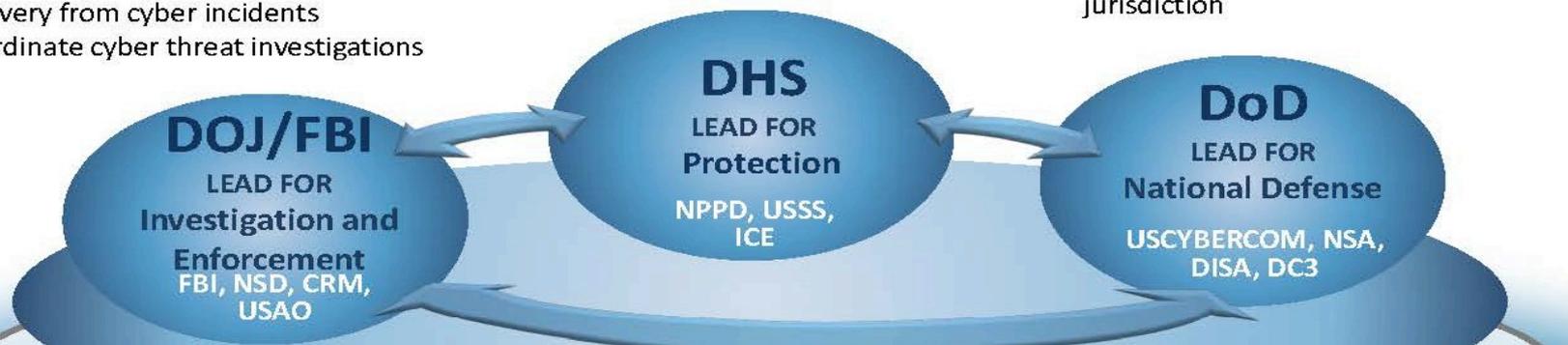
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate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



INTELLIGENCE COMMUNITY: Cyber Threat Intelligence & Attribution
SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS

PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

Coordinate with Public, Private, and International Partners

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

NITRD Participating Agencies



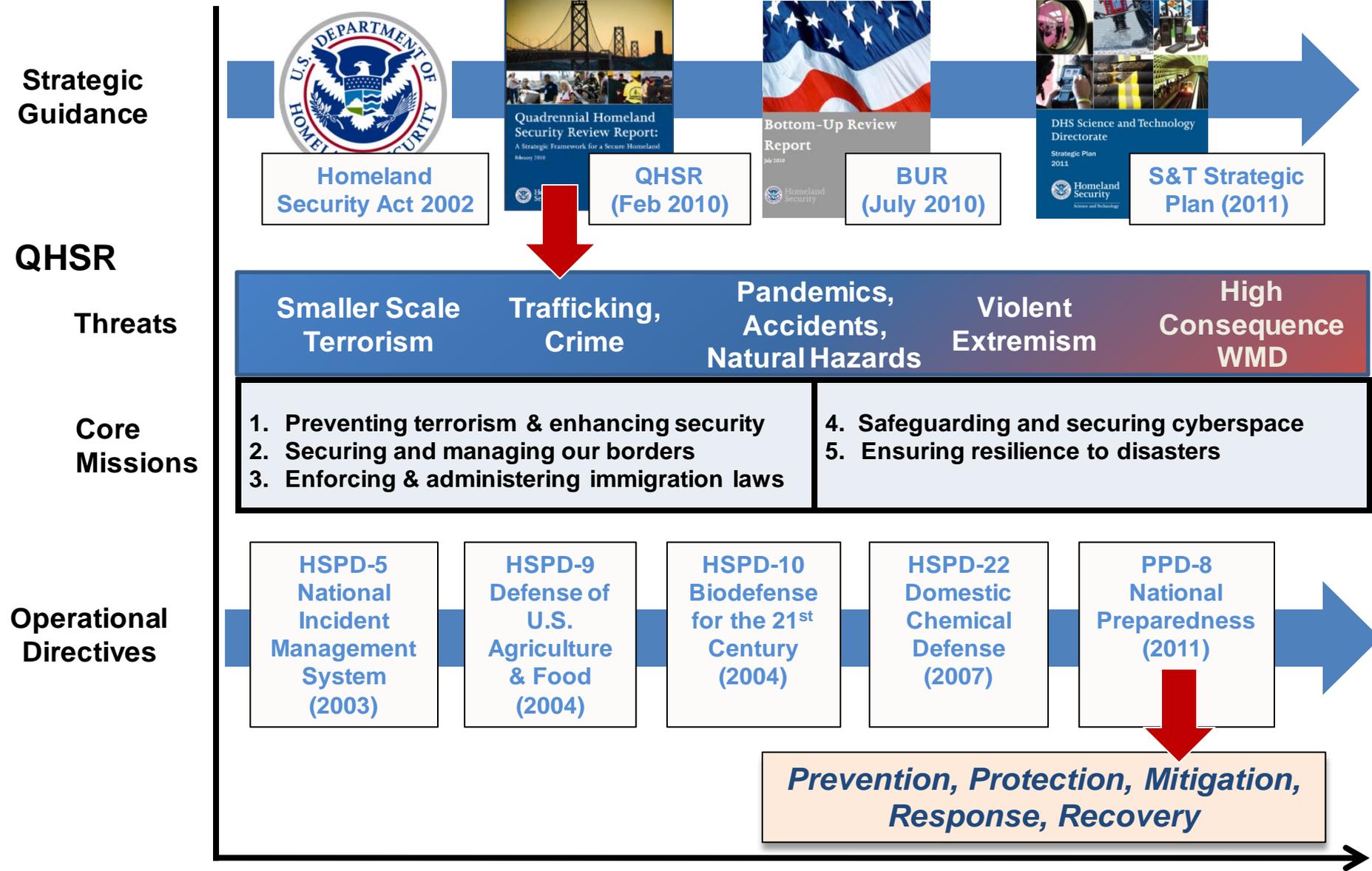
- Science of Cyber Security
- Research Themes
 - Tailored Trustworthy Spaces
 - Moving Target Defense
 - Cyber Economics and Incentives
 - Designed-In Security (New for FY13)
- Transition to Practice
 - Technology Discovery
 - Test & Evaluation / Experimental Deployment
 - Transition / Adoption / Commercialization
- Support for National Priorities
 - Health IT, Smart Grid, NSTIC (Trusted Identity), NICE (Education), Financial Services



Released Dec 6, 2011

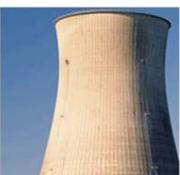
<http://www.whitehouse.gov/blog/2011/12/06/federal-cybersecurity-rd-strategic-plan-released>

DHS S&T Mission Guidance



Cybersecurity for the 16 Critical Infrastructure Sectors

DHS provides advice and alerts to the 16 critical infrastructure areas ...

					
Agriculture & Food	Banking & Finance	Chemical Sector	Comms Sector	Commercial Facilities	Critical Manufacturing
					
Dams	Information Technology	Energy	Government Facilities	Healthcare and Public Health	Water
					
Nuclear Reactors, Materials and Waste	Postal and Shipping	Defense Industrial Base	Transportation Systems	National Monuments Icons	Emergency Services

... DHS collaborates with sectors through Sector Coordinating Councils (SCC)

In the future, DHS will provide cybersecurity for ...

- The .gov and critical .com domains with a mix of:
 - Managed security services
 - Developmental activities
 - Information sharing
- Linkages to our U.S. – CERT (Computer Emergency Readiness Team)

National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center for production of a common operating picture ...



Integrating Cyber-Physical Security

- ***Executive Order 13636: Improving Critical Infrastructure Cybersecurity*** directs the Executive Branch to:
 - Develop a technology-neutral voluntary cybersecurity framework
 - Promote and incentivize the 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 the use of 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 the cascading consequences of infrastructure failures
 - Evaluate and mature the public-private partnership
 - Update the National Infrastructure Protection Plan
 - **Develop comprehensive research and development plan (CSD / RSD)**

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
- Explosives
- Cybersecurity
- First Responders



**Homeland
Security**

Science and Technology



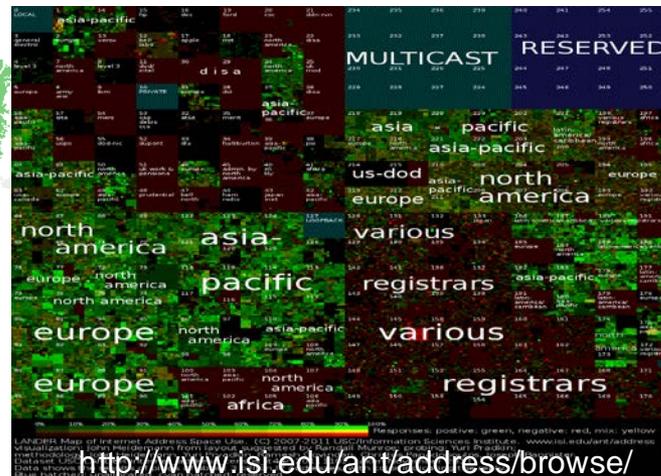
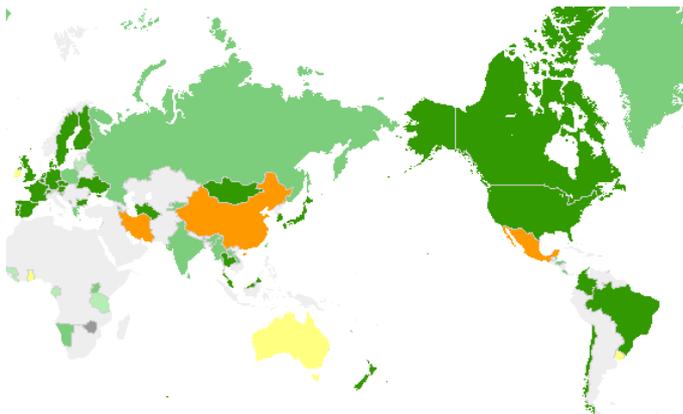
Cyber Security Focus Areas

- Trustworthy Cyber Infrastructure
 - Working with the global Internet community to secure cyberspace
- Research Infrastructure to Support Cybersecurity
 - Developing necessary research infrastructure to support R&D community
- R&D Partnerships
 - Establishing R&D partnerships with private sector, academia, and international partners
- Innovation and Transition
 - Ensuring R&D results become real solutions
- Cybersecurity Education
 - Leading National and DHS cybersecurity education initiatives

Trustworthy Cyber Infrastructure

- Secure Protocols
 - DNSSEC – Domain Name System Security
 - Govt and private sector worked together to make this happen
 - Started in 2004; now 111 top level (gTLD) and country code (ccTLD) domains adopted globally including the Root
 - SPRI – Secure Protocols for Routing Infrastructure
- Internet Measurement and Attack Modeling
 - Geographic mapping of Internet resources
 - Logically and/or physically connected maps of Internet resources
 - Monitoring and archiving of BGP route information
 - Co-funding with Australia

ccTLD DNSSEC Status on 2013-01-29



Research Infrastructure (RISC)

- Experimental Research Testbed (DETER)
 - Researcher and vendor-neutral experimental infrastructure
 - Used by over 200 organizations from more than 20 states and 17 countries
 - Used by over 40 classes, from 30 institutions involving 2,000+ students
 - <http://www.deter-project.org>
- Research Data Repository (PREDICT)
 - Repository of network data for use by the U.S.- based cyber security research community
 - More than 200 users (academia, industry, gov't); Over 600TB of network data; Tools are used by major service providers and many companies
 - Phase 2: New datasets, ICTR Ethics, International (CA, AUS, JP, EU)
 - <https://www.predict.org>
- Software Assurance Market Place (SWAMP)
 - A software assurance testing and evaluation facility and the associated research infrastructure services



R&D Partnerships

- Oil and Gas Sector
 - LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity
- Electric Power Sector
 - TCIPG – Trustworthy Computing Infrastructure for the Power Grid
- Banking and Finance Sector
 - FI-VICS – Financial Institutions – Verification of Identity Credential Service
 - DECIDE – Distributed Environment for Critical Incident Decision-making Exercises (recent Quantum Dawn II exercise)
- State and Local
 - PRISEM - Public Regional Information Security Event Management
 - PIV-I/FRAC TTWG – State and Local and Private Sector First Responder Authentication Credentials and Technology Transition
- Law Enforcement
 - SWGDE – Special Working Group on Digital Evidence (FBI lead)
 - CFWG – Cyber Forensics Working Group (CBP, ICE, USSS, FBI, S/L)



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)

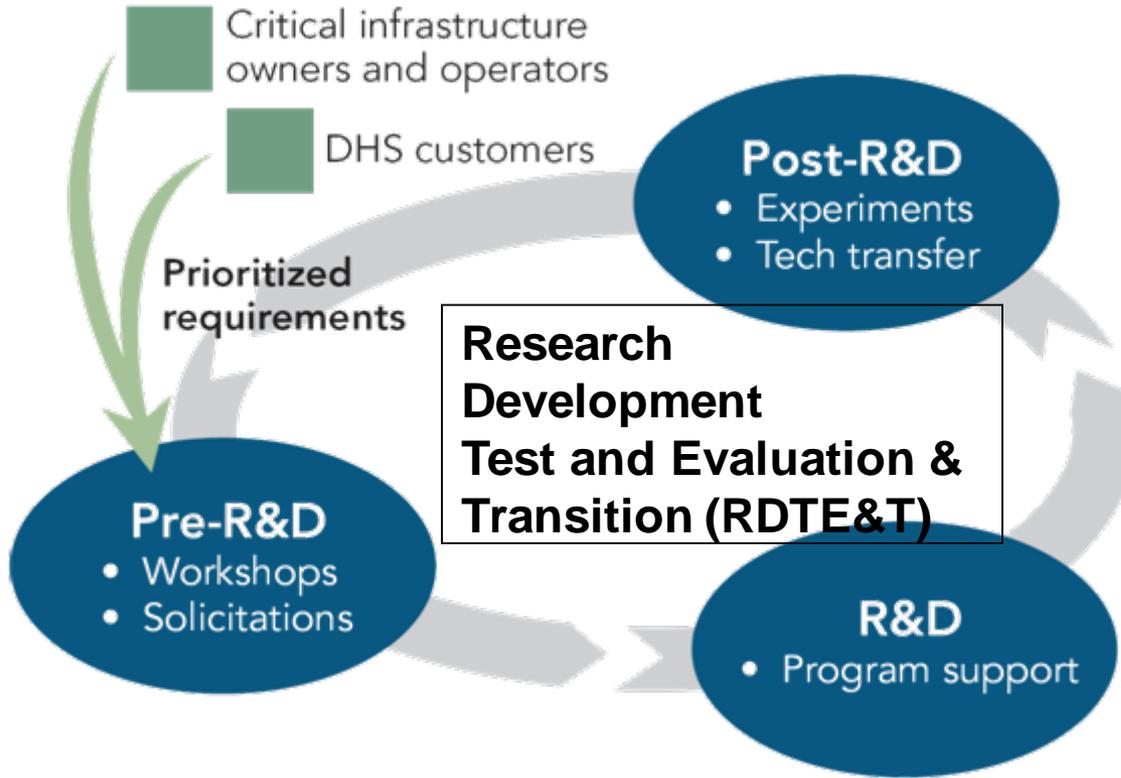


COUNTRY	PROJECTS	MONEY IN	JOINT	MONEY OUT
Australia	3	\$300K	\$400K	
Canada	11	\$1.8M		
Germany	1		\$300K	
Israel	2		\$100K	
Netherlands	7	\$450K	\$1.2M	\$150K
Sweden	4	\$650K		
United Kingdom	3	\$1.2M	\$400K	
European Union	1			
Japan	1			

Over \$6M of International co-funding



CSD R&D Execution Model



Successes

- Ironkey – Secure USB
 - Standard Issue to S&T employees from S&T CIO
 - Acquired by Imation
- Komoku – Rootkit Detection Technology
 - Acquired by Microsoft
- HBGary – Memory and Malware Analysis
 - Over 100 pilot deployments as part of Cyber Forensics
- Endeavor Systems – Malware Analysis tools
 - Acquired by McAfee
- Stanford – Anti-Phishing Technologies
 - Open source; most browsers have included Stanford R&D
- Secure Decisions – Data Visualization
 - Pilot with DHS/NCSD/US-CERT; Acquisition

Example: DARPA has provided \$9M to CSD for development and transition of Military Networking Protocol (MNP) technology and has started discussions for testing and evaluation of Automated Malware Analysis technology

Transition To Practice (TTP) Program



R&D Sources

- **DOE National Labs**
- **FFRDC's** (Federally Funded R&D Centers)
- **Academia**
- **Small Business**

Transition processes

- **Testing & evaluation**
- **Red Teaming**
- **Pilot deployments**

Utilization

- **Open Sourcing**
- **Licensing**
- **New Companies**
- **Adoption by cyber operations analysts**
- **Direct private-sector adoption**
- **Government use**

- ❑ Implement Presidential Memorandum – “Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses” (Oct 28, 2011)

Cyber Security R&D Broad Agency Announcement (BAA)

- Delivers both near-term and medium-term solutions
 - To **develop new and enhanced technologies** for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure, based on customer requirements
 - To perform research and development (R&D) aimed at **improving the security of existing deployed technologies** and to ensure the security of new emerging cybersecurity systems;
 - To **facilitate the transfer of these technologies** into operational environments.
- Proposals Received According to 3 Levels of Technology Maturity

Type I (New Technologies)

- ✓ Applied Research Phase
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ \$3M & 36 mos.

Type II (Prototype Technologies)

- ✓ More Mature Prototypes
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ \$2M & 24 mos.

Type III (Mature Technologies)

- ✓ Mature Technology
- ✓ Demo Only in Op Environ.
- ✓ Funding ≤ \$750K & 12 mos.

Note: Technology Demonstrations = Test, Evaluation, and Pilot deployment in DHS "customer" environments



**Homeland
Security**

Science and Technology

BAA 11-02 Technical Topic Areas (TTAs)

TTA-1	Software Assurance	DHS, FSSCC
TTA-2	Enterprise-Level Security Metrics	DHS, FSSCC
TTA-3	Usable Security	DHS, FSSCC
TTA-4	Insider Threat	DHS, FSSCC
TTA-5	Resilient Systems and Networks	DHS, FSSCC
TTA-6	Modeling of Internet Attacks	DHS
TTA-7	Network Mapping and Measurement	DHS
TTA-8	Incident Response Communities	DHS
TTA-9	Cyber Economics	CNCI
TTA-10	Digital Provenance	CNCI
TTA-11	Hardware-Enabled Trust	CNCI
TTA-12	Moving Target Defense	CNCI
TTA-13	Nature-Inspired Cyber Health	CNCI
TTA-14	Software Assurance MarketPlace (SWAMP)	S&T



**Homeland
Security**

Science and Technology

- 1003 White Papers
- 224 Full Proposals encouraged
- 34 Awards – Sep/Oct 2012

- Int'l participation from AUS, UK, CA, NL, SWE
- Over \$4M of joint funding

BAA 11-02 Winning Awards

Applied Visions, Inc	Oak Ridge National Laboratory
Carnegie-Mellon University	Pacific NW National Laboratory
Columbia University	Purdue University
Def-Logix	Raytheon BBN Technologies
George Mason University	Rutgers University
Georgia Tech Research Corp.	Princeton University
HRL Laboratories, LLC	University of Alabama at Birmingham
IBM Research	University of North Carolina
International Computer Science Institute	Dartmouth College
ITT Exelis	Indiana University
Kestrel Technology, LLC	University of California, San Diego
Merit Network Inc	University of Houston
Morgridge Institute for Research	University of Illinois at Urbana-Champaign
Naval Postgraduate School	University of Maryland
Northrop Grumman Information Systems	USC Information Sciences Institute

Cybersecurity Education

- **Cyber Security Competitions (<http://nationalccdc.org>)**
 - National Initiative for Cybersecurity Education (NICE)
 - NCCDC (Collegiate); U.S. Cyber Challenge (High School)
 - Provide a controlled, competitive environment to assess a student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.

- **DHS Cyber Skills Task Force (CSTF)**
 - Established June 6, 2012 - Homeland Security Advisory Council
 - Over 50 interviews (DHS internal and external)
 - Identify best ways DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges;
 - Outline how DHS can improve its capability to recruit and retain sophisticated cybersecurity talent.
 - 11 recommendations in 5 key areas





Summary

- Cybersecurity research is a key area of innovation to support our global economic and national security futures
- DHS S&T continues with an aggressive cyber security research agenda
 - Working to solve the cyber security problems of our current (and future) infrastructure and systems
 - Working with academe and industry to improve research tools and datasets
 - Looking at future R&D agendas with the most impact for the nation
- Need to continue strong emphasis on technology transfer and experimental deployments
- Must focus on the education, training, and awareness aspects of our current and future cybersecurity workforce



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.cyber.st.dhs.gov>

<http://www.dhs.gov/st-csd>



Homeland Security

Science and Technology