

Homeland Security Advanced Research Projects Agency

Cyber Security Division Overview

Douglas Maughan, Ph.D.
Director

October 9, 2012



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



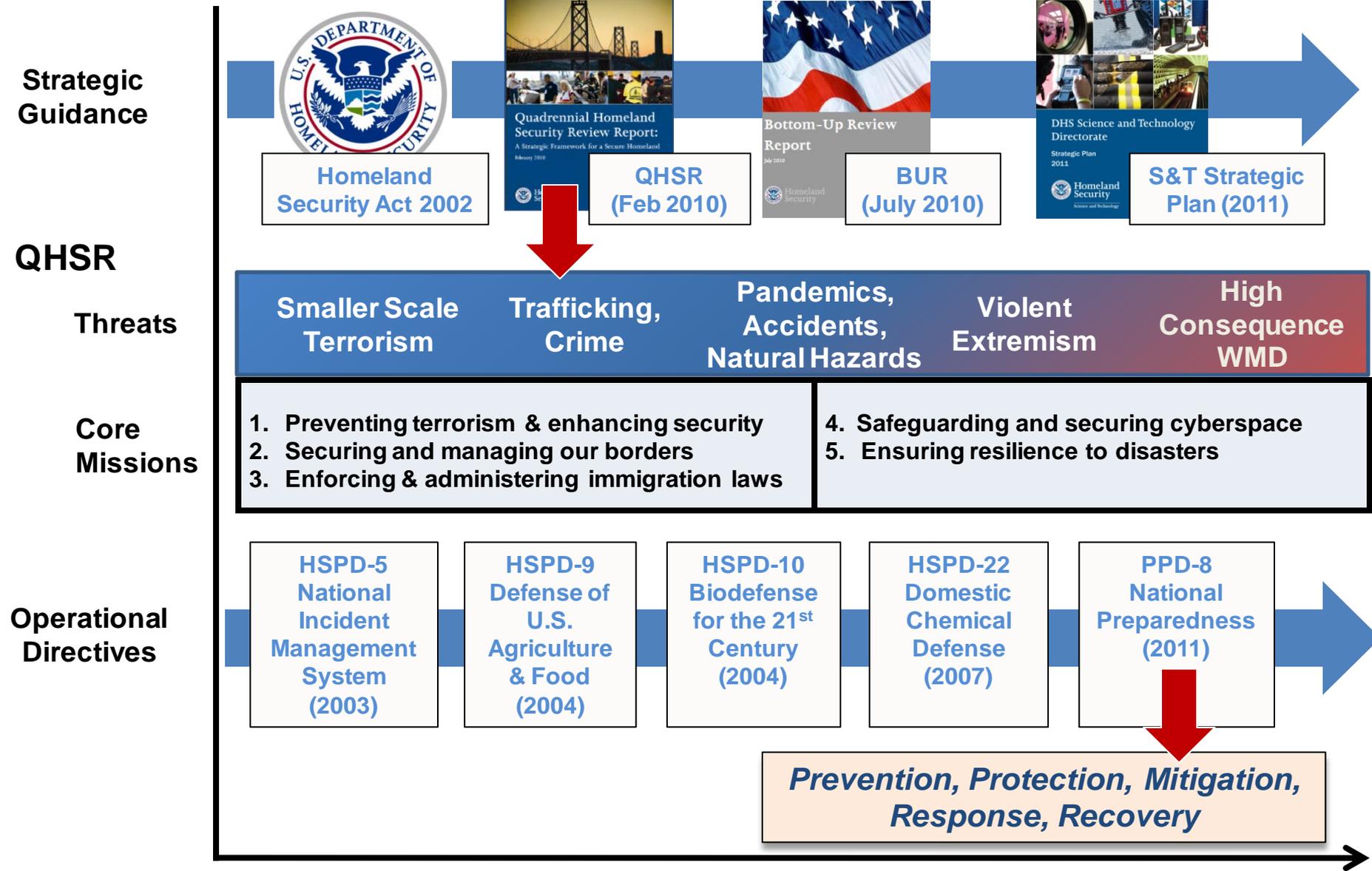
Homeland Security

Science and Technology

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



DHS S&T Mission Guidance





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
Redirect S&T 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
S&T CSD not involved

Develop Gov't-wide Counterintelligence

Enhance Security of the Classified Networks

NICE – S&T involved
Expand Education

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

Focus Area 3

S&T – \$18M FY12 OMB add

Define and Develop Enduring Deterrence Strategies & Programs

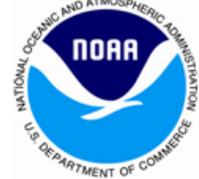
Inter-agency Programs
S&T CSD not involved

Manage Global Supply Chain Risk

NIPP – S&T involved
Critical Infrastructure Domains



Federal Cybersecurity Research and Development Program: Strategic Plan



Homeland Security



Science and Technology



Federal Cybersecurity R&D Strategic Plan



- Science of Cyber Security
- Research Themes
 - Tailored Trustworthy Spaces
 - Moving Target Defense
 - Cyber Economics and Incentives
 - Designed-In Security (New for FY12)
- 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

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



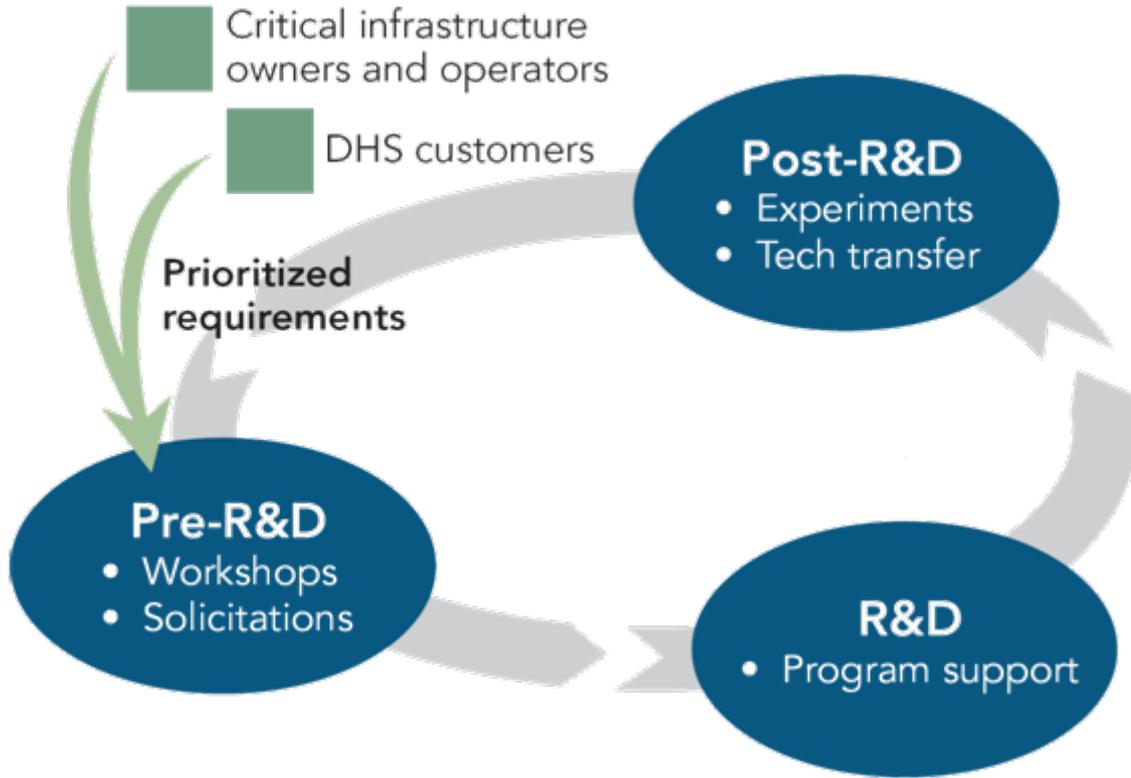
**Homeland
Security**

Science and Technology





CSD R&D Execution Model



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

Successes

- Ironkey – Secure USB
 - Standard Issue to S&T employees from S&T CIO
- 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

Cyber Security Program Areas

- Research Infrastructure to Support Cybersecurity (RISC)
- Trustworthy Cyber Infrastructure (TCI)
- Foundational Elements of Cyber Systems (FECS)
- Cybersecurity User Protection and Education (CUPE)
- Cyber Technology Evaluation and Transition (CTET)



**Homeland
Security**

Science and Technology

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 5TB 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
 - New FY12 initiative



**Homeland
Security**

Science and Technology

Trustworthy Cyber Infrastructure

- Secure Protocols
 - DNSSEC – Domain Name System Security
 - Govt and private sector worked together to make this happen
 - Started in 2004; now 35 top level domains adopted globally including the Root
 - SPRI – Secure Protocols for Routing Infrastructure
- Process Control Systems
 - LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity
 - Consortium of 5 super major O&G companies partnered with DHS
 - TCIPG – Trustworthy Computing Infrastructure for the Power Grid
 - Partnered with DOE, Advisory Board of 30+ private sector companies
- 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



Foundational Elements (FECS)

- Enterprise Level Security Metrics and Usability
- Homeland Open Security Technology (HOST)
- Software Quality Assurance
 - S2ERC – Security and Software Engineering Research Center
- Cyber Economic Incentives (CNCI)
 - New FY12 Initiative
- Leap Ahead Technologies (CNCI)
- Moving Target Defense (CNCI)
 - New FY12 Initiative
- Tailored Trustworthy Spaces (CNCI)
 - New FY12 Initiative



**Homeland
Security**

Science and Technology

Cybersecurity Users (CUPE)

- Cyber Security Competitions
 - National Initiative for Cybersecurity Education (NICE)
 - NCCDC (Collegiate); U.S. Cyber Challenge (High School)
- Cyber Security Forensics
 - Support to DHS and other Law Enforcement customers (USSS, CBP, ICE, FBI, CIA)
- Identity Management & Data Privacy Technologies
 - National Strategy for Trusted Identities in Cyberspace (NSTIC)



**Homeland
Security**

Science and Technology

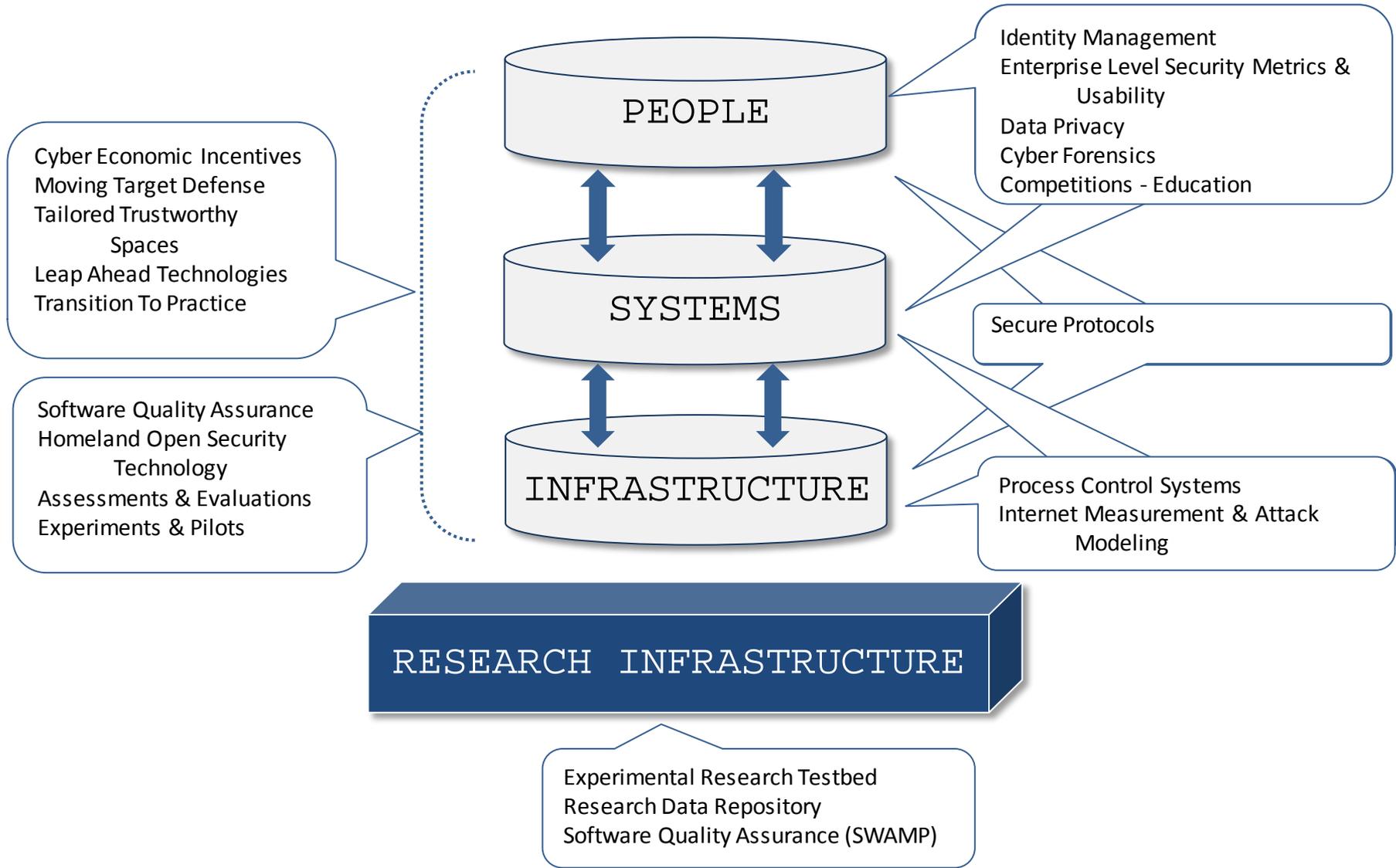
Evaluation and Transition (CTET)

- Assessment and Evaluations
 - Red Teaming of DHS S&T-funded technologies
 - Support of the Security Innovation Network (SINET)
 - Annual IT Security Entrepreneurs' Forum
 - Quarterly Information Security Technology Transition Council (ITTC) meetings
- Experiments and Pilots
 - Experimental Deployment of DHS S&T-funded technologies into operational environments
 - Partnerships with ICE, USSS, CBP, NCSD, S&T CIO
 - Distributed Environment for Critical Incident Decision-making Exercises (DECIDE) Tool for Finance Sector to conduct risk management exercises and identify improvements
- Transition to Practice (CNCI)
 - New FY12 Initiative





CSD Programs and Relationships - Across Layers



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.



**Homeland
Security**

Science and Technology

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

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



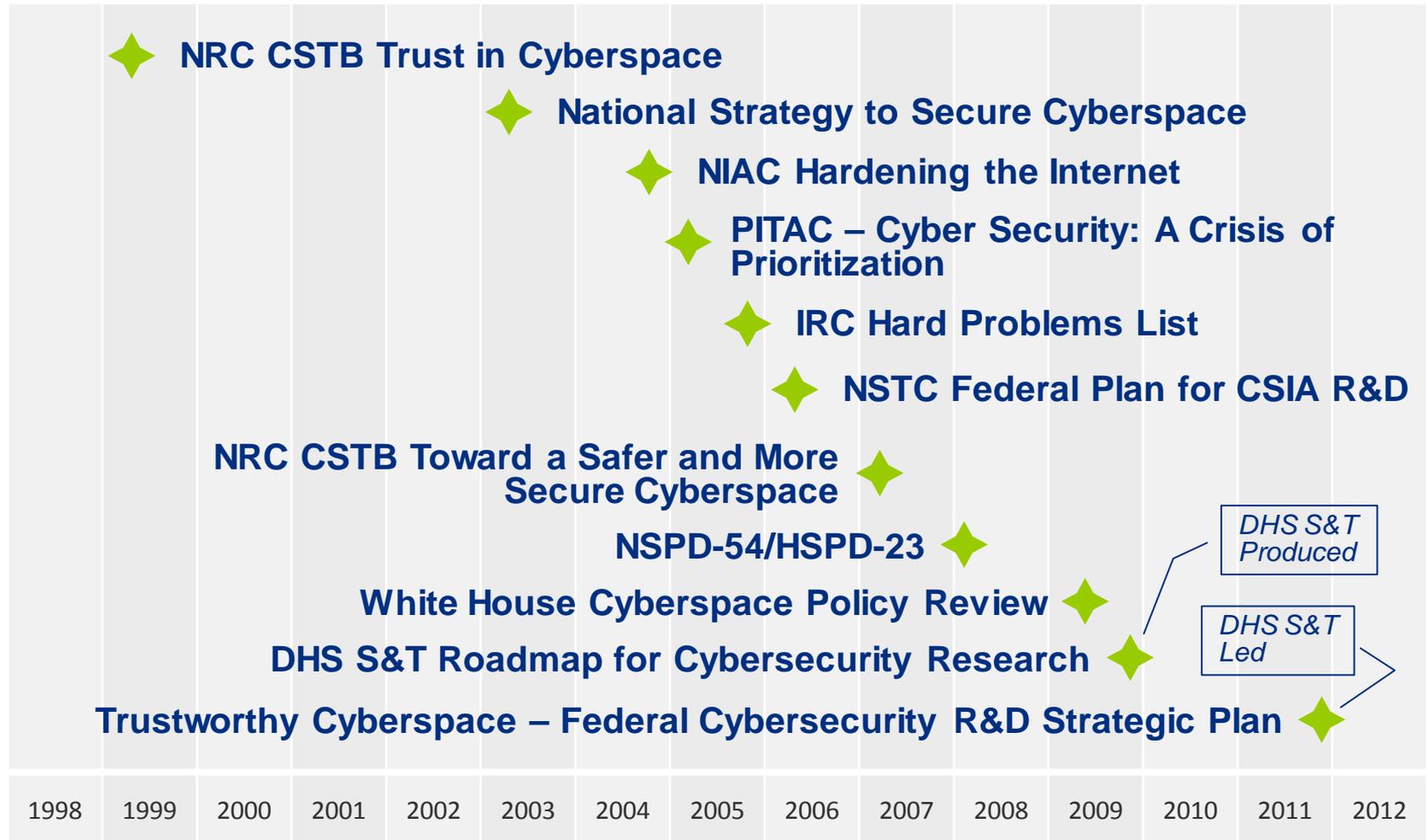
**Homeland
Security**

Science and Technology

- 1003 White Papers
- 224 Full Proposals encouraged

- Int'l participation from AUS, UK, CA, NL, SWE

History of National Cyber Security Work



Homeland Security

Science and Technology

All documents available at:
<http://www.cyber.st.dhs.gov/resources/>

A Roadmap for Cybersecurity Research

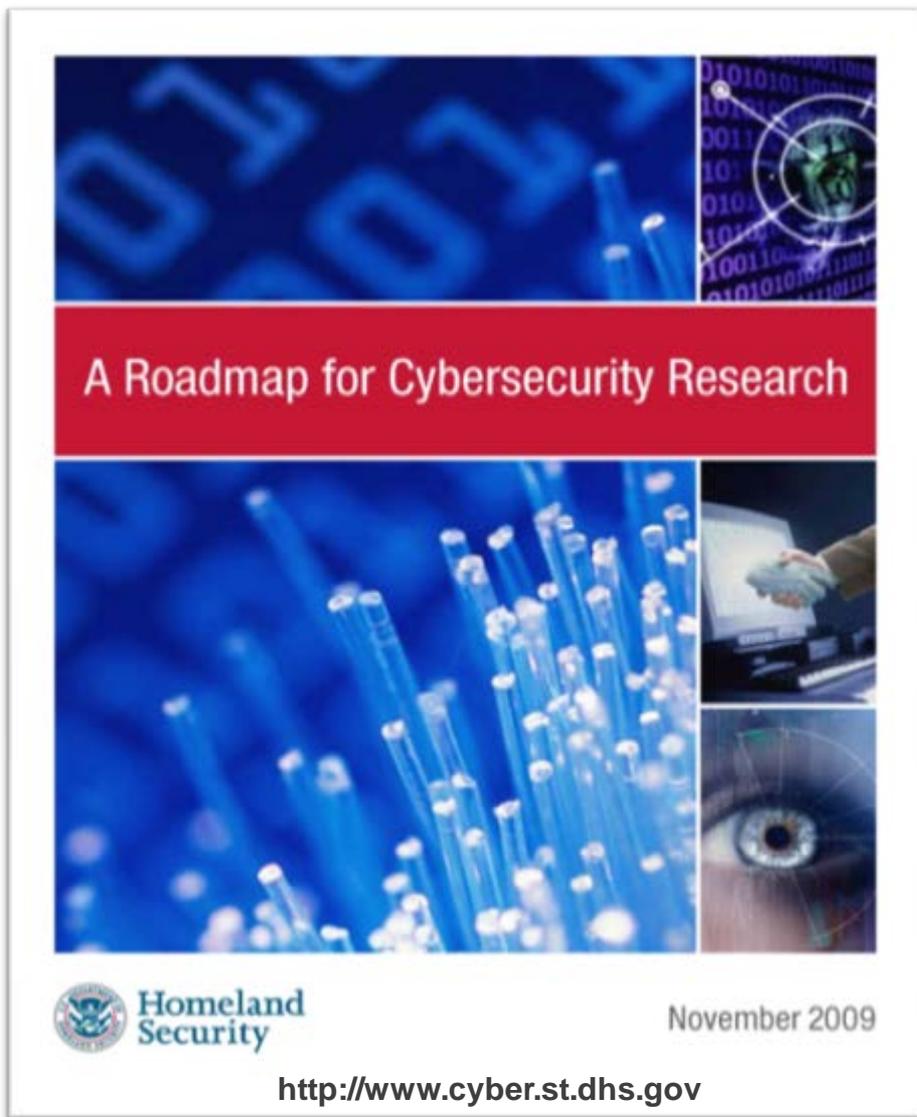
Identified critical research gaps in:

- Scalable Trustworthy Systems
- Enterprise Level Metrics
- System Evaluation Lifecycle
- Combating Insider Threats
- Combating Malware and Botnets
- Global-Scale Identity Management
- Survivability of Time-Critical Systems
- Situational Understanding and Attack Attribution
- Information Provenance
- Privacy-Aware Security
- Usable Security



**Homeland
Security**

Science and Technology



 **Homeland
Security**

November 2009

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



FY2011 Annual Report



Cyber Security Division

FY 2011 Annual Report



Homeland
Security

Science and Technology



Summary

- Cybersecurity research is a key area of innovation needed to support our future
- 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, including education
- Need to continue strong emphasis on technology transfer and experimental deployments



**Homeland
Security**

Science and Technology

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>



**Homeland
Security**

Science and Technology

Guidance for PI Presentations

- Briefing Format
 - Intro: TTA you are addressing and team make up: 1-2 minutes
 - Technical Approach: 6-8 minutes
 - Discuss problem, solution, and technical challenges
 - Milestones, Deliverables, and Schedule: 3-4 minutes
 - Highlight reports, papers, software, etc.
 - Technology Transition Plan: 2-3 minutes
 - Specify what it would take to get to a pilot; Using DETER and/or PREDICT?
 - Quad Chart (remove any budget numbers)
- Slide Formats - Use Presentation Format provided
- Presentation Timing – Countdown Timer
 - Actual time is 15 minutes – 5 minutes for Q&A and transition
- **NO** questions during presentations
 - Save them for the end or talk during the breaks



PI Meeting Expectations

- Rule #1: Expect all to participate, ask questions, provide feedback (both online and offline – use tact)
- Rule #2: Take opportunities to talk with others about collaborative opportunities
 - Five international partners (AUS, CA, NL, SW, UK) that are interested in co-funding your work
 - Especially interested in identifying possible experiments with integration of multiple technologies
 - Including identification of possible end customers
- Rule #3: Comments/Critique of agenda
 - **ACTION:** If you have other ideas for format, content, etc., please let me know.



Administrative Information

- Provide copies of your project briefings to Matthew Billone (Matthew.Billone@associates.hq.dhs.gov) by the end of the day before your briefing. Final briefings will be posted on the CSD website within a week.
- Performers must complete/send their deliverables on time, especially the monthly financial status reports.....
No deliverables, then no money.
- Type I and Type II contracts, due to the Continuing Resolution (CR) funds may be awarded in increments this year, please work with your Contracting Agency and DHS S&T POCs to keep current on expenditures/funds status. You have a requirement in your contract to let us know when you've spent 75% of the funds. PLEASE make sure you notify us. EMERGENCIES UNALLOWED



**Homeland
Security**

Science and Technology

Administrative Information (continued)

- All technical and financial reports must be submitted to your COR and SandT-Cyber-Reports@hq.dhs.gov.
- Each report submitted to Cyber Reports mailbox shall have in the subject line of the email the organization name, contract number, and report description as follows:
 - AFRL issued awards example:
 - Organization X FA8750120000 Quarterly Technical Report
 - SSC PACIFIC issued awards example:
 - Organization X N6600112C0000 Quarterly Technical Report
 - Do not include any dashes in the contract number.



**Homeland
Security**

Science and Technology

Administrative Information (continued)

- Project Abstracts
 - DHS S&T will be posting project abstracts, similar to what is typically done by NSF
 - We will be working with you over the next month or two to get a final version completed and posted
- PI meetings
 - Intermediate (6-month) PI meeting – Ask your Program Manager
 - Next “Full” PI Meeting – Still TBD, but plan on October 2013
- PR – Public Relations and/or Press Releases
 - DHS S&T PR announcement will be released next week; you are then free to do your own, but coordinate with your PM. If you mention DHS S&T (which you should), then we need to see it
 - Anytime you have something that appears in the press, please send a notification to your PM and SETA

