

# Homeland Security Advanced Research Projects Agency

## Cyber Security Division

*Douglas Maughan, Ph.D.*  
*Director*

*July 26, 2012*



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

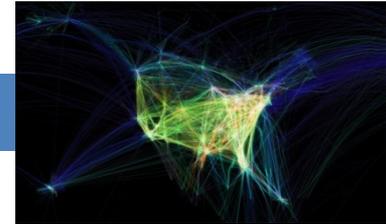
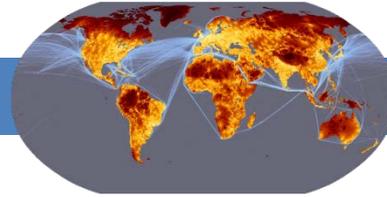


# Homeland Security

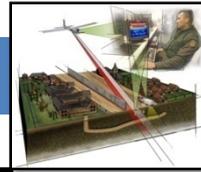
Science and Technology

# Greater Use of Technology, More Threats

**Globalization & Transportation**



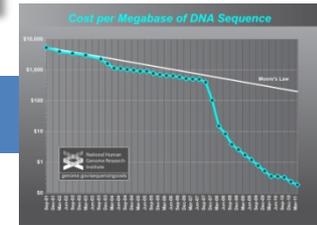
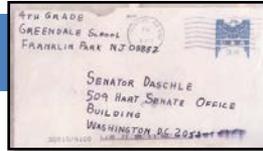
**Border Security & Immigration**



**Violent Extremism**



**Misuse of Technology**

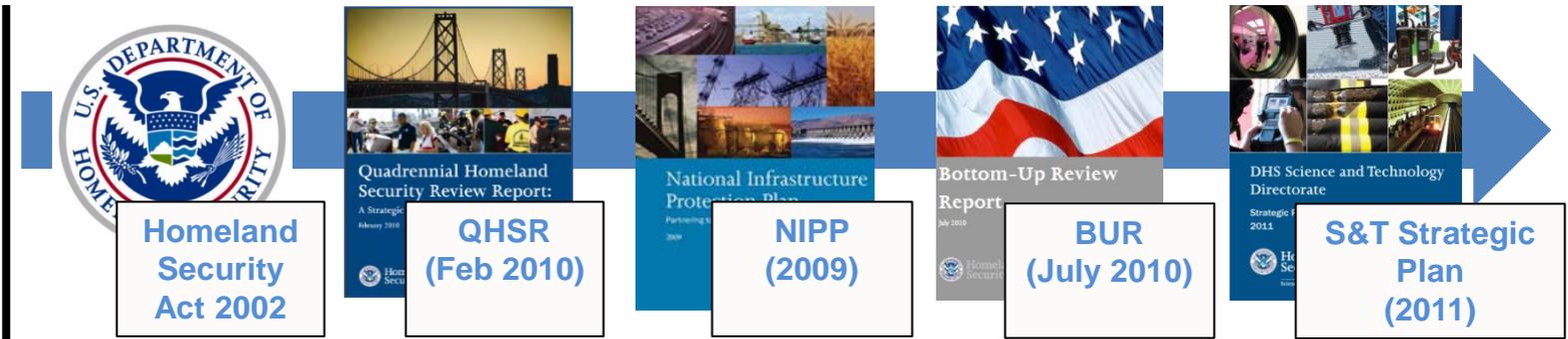


**Natural Disasters & Pushing Beyond Design Limits**



# DHS S&T Mission Guidance

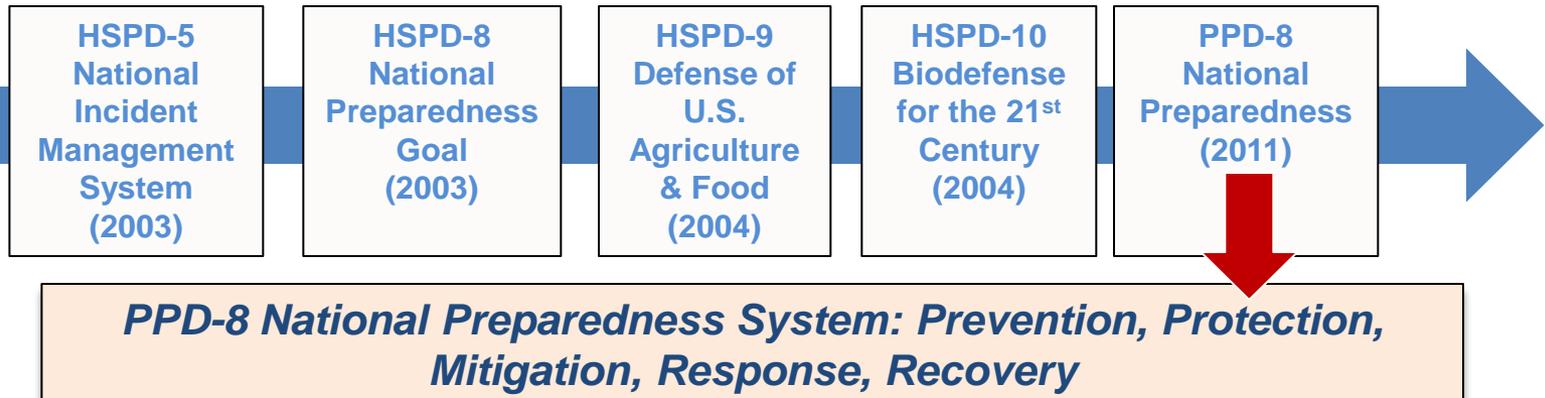
## Strategic Guidance



## DHS Core Missions

1. Preventing terrorism & enhancing security
2. Securing and managing our borders
3. Enforcing and administering our immigration laws
4. **Safeguarding and securing cyberspace**
5. Ensuring resilience to disasters
6. Maturing & Strengthening the Homeland Security Enterprise

## Operational Directives



# Comprehensive National Cybersecurity Initiative (CNCI)

Focus Area 1

## Establish a front line of defense

Reduce the Number of Trusted Internet Connections

Deploy Passive Sensors Across Federal Systems

Pursue Deployment of Automated Defense Systems

Coordinate and Redirect R&D Efforts

Focus Area 2

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

Connect Current Centers to Enhance Situational Awareness

Develop Gov't-wide Counterintelligence Plan for Cyber

Increase Security of the Classified Networks

Expand Education

Focus Area 3

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

Define and Develop Enduring Leap Ahead Technologies, Strategies & Programs

Define and Develop Enduring Deterrence Strategies & Programs

Manage Global Supply Chain Risk

Cyber Security in Critical Infrastructure Domains



**Homeland Security**

Science and Technology

<http://cybersecurity.whitehouse.gov>

# Federal Cybersecurity R&D Strategic Plan

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



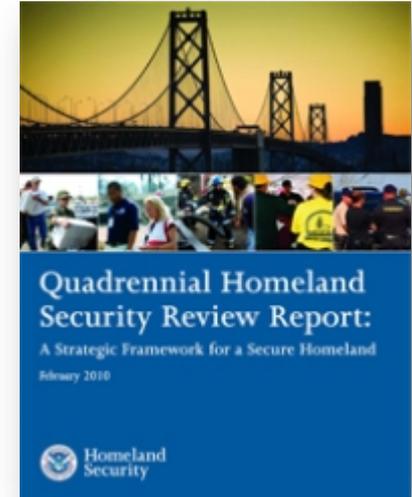
**Homeland  
Security**

Science and Technology

# Quadrennial Homeland Security Review

## DHS Core Missions

- 1) Preventing terrorism and enhancing security
- 2) Securing and managing our borders
- 3) Enforcing and administering our immigration laws
- 4) **Safeguarding and securing cyberspace**
  - Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment*
  - Goal 4.2: Promote Cybersecurity Knowledge and Innovation*
- 5) Ensuring resilience to disasters



## Maturing and strengthening the Homeland Security Enterprise

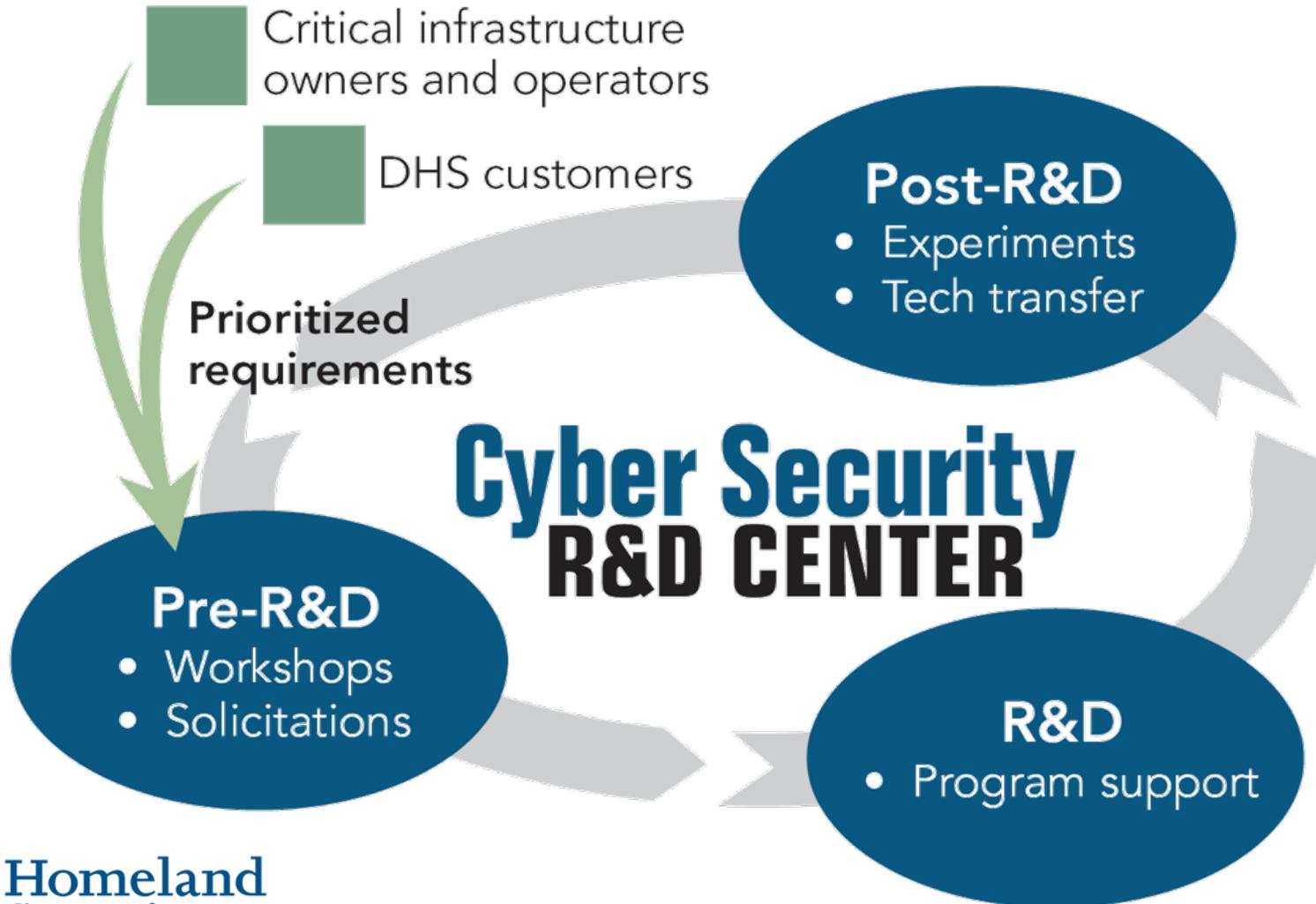
- *Foster Innovative Approaches and Solutions Through Leading-Edge Science and Technology*



**Homeland  
Security**

Science and Technology

# CSD R&D Execution Model



**Homeland Security**

Science and Technology

# Examples of CSD Successes

- Ironkey – Secure USB
  - Standard Issue to S&T employees from S&T CIO
- Coverity – Open Source Hardening (SCAN)
  - Analyzes 150+ open source software packages daily
- Komoku – Rootkit Detection Technology
  - Acquired by Microsoft in 2008
- Secure64 – DNSSEC Automation
- HBGary – Memory and Malware Analysis
  - Over 100 pilot deployments as part of Cyber Forensics project
- Endeavor Systems – Malware Analysis tools
  - Acquired by McAfee in 2009
- Telcordia – Automated Vulnerability Analysis
  - In use by DOD, SEC
- GMU/ProInfo – Network Topology Analysis (Cauldron)
  - In use at FAA, several commercial customers
- Stanford – Anti-Phishing Technologies
  - Open source; most browsers have included Stanford R&D



- Secure Decisions – Data Visualization
  - Pilot with DHS/NCSD/US-CERT



**Homeland  
Security**

Science and Technology

# 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



**Homeland  
Security**

Science and Technology

# Foundational Elements (FECS)

- Enterprise Level Security Metrics and Usability
- Homeland Open Security Technology (HOST)
- Software Quality Assurance
- 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)



the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG PHOTOS & VIDEO BRIEFING ROOM ISSUES the ADMINISTRATION

Home • The Administration • Office of Science and Technology Policy

 Office of Science and Technology Policy

About OSTP | OSTP Blog | Pressroom | Divisions | R&D Budgets | Resource Library | NSTIC

### Partnership for Cybersecurity Innovation

Posted by [Aneesh Chopra](#) and [Howard A. Schmidt](#) on December 06, 2010 at 03:04 PM EST

Today, Obama Administration officials released a [Memorandum of Understanding](#) signed by the National Institute of Standards and Technology (NIST) of the Department of Commerce, the Science and Technology Directorate of the Department of Homeland Security (DHS/S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our Nation's critical infrastructures.

The agreement establishes a framework for collaboration between the public and private sectors as directed by President Obama in his [cybersecurity policy address](#):

*"We will collaborate with industry to find technology solutions that ensure our security and promote prosperity."*

- President Obama, May 29, 2009



**Homeland  
Security**

Science and Technology

# Evaluation and Transition (CTET)

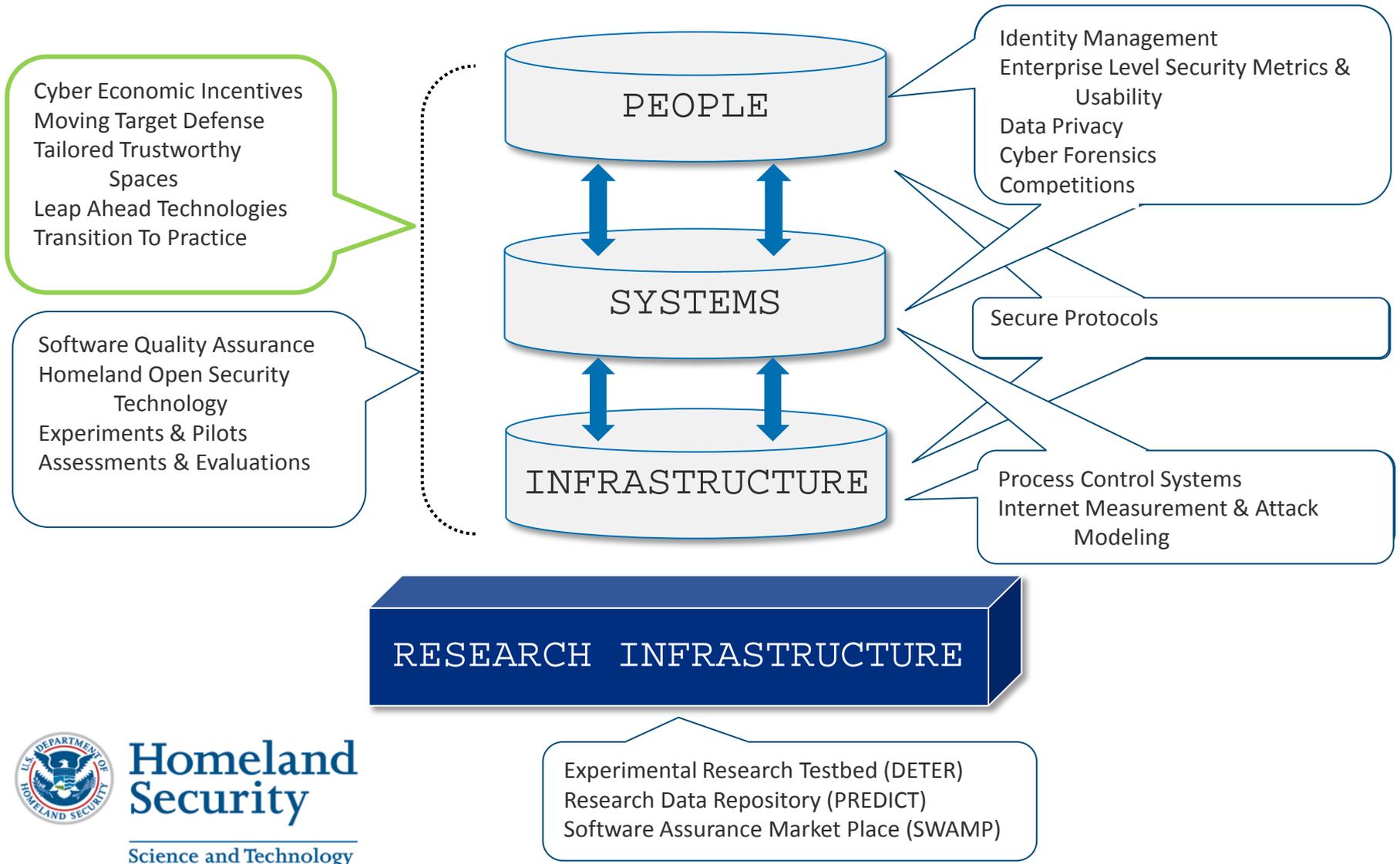
- Assessment and Evaluations
  - Red Teaming of DHS S&T-funded technologies
  - Support of the Security Innovation Network (SINET)
    - Annual IT Security Entrepreneurs' Forum
    - Quarterly Information Security Technology Transition Council (ITTC) meetings
- Experiments and Pilots
  - Experimental 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



**Homeland  
Security**

Science and Technology

# DHS S&T Cybersecurity Program



**Homeland Security**

Science and Technology

# 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
- Expected awards in Jun/Jul 2012

# Small Business Innovative Research (SBIR)

---

- FY04
  - Cross-Domain Attack Correlation Technologies (2)
  - Real-Time Malicious Code Identification (2)
  - Advanced SCADA and Related Distributed Control Systems (5)
- FY05
  - Hardware-assisted System Security Monitoring (4)
- FY06
  - Network-based Boundary Controllers (3)
  - Botnet Detection and Mitigation (4)
- FY07
  - Secure and Reliable Wireless Communication for Control Systems (2)
- FY09
  - Software Testing and Vulnerability Analysis (3)
- FY10
  - Large-Scale Network Survivability, Rapid Recovery, and Reconstitution (1)
- FY11
  - Mobile Device Forensics (1)
- FY12
  - Moving Target Defense (CNCI Topic)
  - Solid State Drive Analysis



# Small Business Innovative Research (SBIR)

- Important program for creating new innovation and accelerating transition into the marketplace
- Since 2004, DHS S&T Cyber Security has had:
  - 63 Phase I efforts
  - 28 Phase II efforts
  - 5 Phase II efforts currently in progress
  - 9 commercial/open source products available
  - Four acquisitions
    - Komoku, Inc. (MD) acquired by Microsoft in March 2008
    - Endeavor Systems (VA) acquired by McAfee in January 2009
    - Solidcore (CA) acquired by McAfee in June 2009
    - HBGary (CA) acquired by ManTech in February 2012



**Homeland  
Security**

Science and Technology

# DHS S&T Long Range Broad Agency Announcement (LRBAA) 12-07

- S&T seeks R&D projects for revolutionary, evolving, and maturing technologies that demonstrate the potential for significant improvement in homeland security missions and operations
- Offerors can submit a pre-submission inquiry prior to White Paper submission that is reviewed by an S&T Program Manager
- CSD has 14 Topic Areas (CSD.01 – CSD.14) – SEE NEXT SLIDE
- LRBAA 12-07 Closes on 12/31/12 at 11:59 PM
- S&T BAA Website: <https://baa2.st.dhs.gov>
- Additional information can be found on the Federal Business Opportunities website ([www.fbo.gov](http://www.fbo.gov)) (Solicitation #:DHSS-TLRBAA12-07)



**Homeland  
Security**

Science and Technology

# LRBAA Summary Listing

- **CSD.01** – Comprehensive National Cybersecurity Initiative and Federal R&D Strategic Plan topics
- **CSD.02** – Internet Infrastructure Security
- **CSD.03** – National Research Infrastructure
- **CSD.04** – Homeland Open Security Technology
- **CSD.05** – Forensics support to law enforcement
- **CSD.06** – Identity Management
- **CSD.07** – Data Privacy and Information Flow technologies.
- **CSD.08** – Software Assurance
- **CSD.09** – Cyber security competitions and education and curriculum development.
- **CSD.10** – Process Control Systems and Critical Infrastructure Security
- **CSD.11** – Internet Measurement and Attack Modeling
- **CSD.12** – Securing the mobile workforce
- **CSD.13** - Security in cloud based systems
- **CSD.14** – Experiments – Technologies developed through federally funded research requiring test and evaluation in experimental operational environments to facilitate transition.



# 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

The cover of the report "A Roadmap for Cybersecurity Research" features a collage of images: a blue background with binary code and a globe, a red banner with the title, a close-up of fiber optic cables, a hand holding a computer mouse, and a close-up of a human eye. The U.S. Department of Homeland Security logo is in the bottom left, and the date "November 2009" is in the bottom right. The URL "http://www.cyber.st.dhs.gov" is at the bottom center.

**A Roadmap for Cybersecurity Research**

November 2009

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

# 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