Homeland Security Advanced Research Projects Agency

Homeland Security – An Overview and Cybersecurity R&D

Douglas Maughan, Ph.D.

Director

October 18, 2012

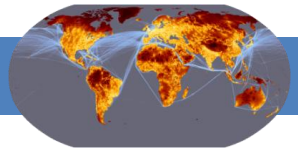
Homeland Security

Science and Technology

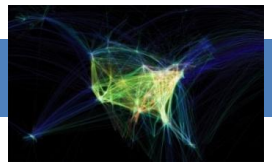
Homeland Security
Science and Technology

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

Globalization & Transportation

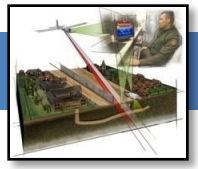


Anywhere in the world in 24 hours

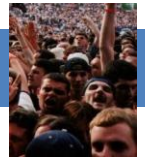


Border Security & Immigration

Tenuous balance



Violent Extremism



Insider Threat

Cyber Domain

Low cost of entry

Strategic potential

Nature of Innovation

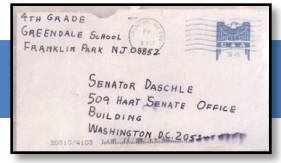
Both sides get to innovate

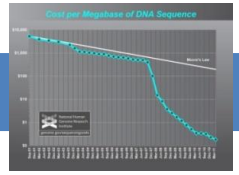
Predictive & Reactive

Aviation as an example …

Misuse of Technology

Historical Perspective





Natural Disasters & Pushing Beyond Design Limits

LESS RESOURCES

MORE THREATS

Homeland Security
Science and Technology

September 2012 Cyber Events

Data breach at IEEE.org: 100k plaintext passwords - 09/25/2012

Worm hitting Saudi - Looks to be very limited and targeted - 09/13/2012

Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent - *09/25/2012*

Iran blamed for cyberattacks on U.S. banks and companies - 9/24/2012

Secret account in mission-critical router opens power plants to tampering - 9/5/2012

Unknown amount of Tiffany & Co. employees' account information exposed by unauthorized access to JPMorgan Chase Bank's servers - 9/5/12

Galaxy S3 hacked via NFC at Mobile Pwn2Own competition - 9/19/12

Mozilla releases patches for more than 30 Firefox bugs - 9/1/12

Security experts hack and refresh US transit cards with Android app - 9/21/12

Twitter users dealt malicious links via direct messages - 9/26/12

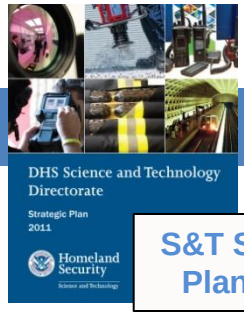
2,500 involved in Kentucky healthcare data breach - 9/19/12

DDoS attacks hit Wells Fargo, PNC Bank, U.S. Bancorp - 9/27/12

Homeland Security
Science and Technology

DHS S&T Mission Guidance

Strategic Guidance



Homeland Security Act 2002 → QHSR (Feb 2010) → BUR (July 2010) → S&T Strategic Plan (2011)

QHSR

Threats

Smaller Scale Terrorism | Trafficking, Crime | Pandemics, Accidents, Natural Hazards | Violent Extremism | High Consequence WMD

Core Missions

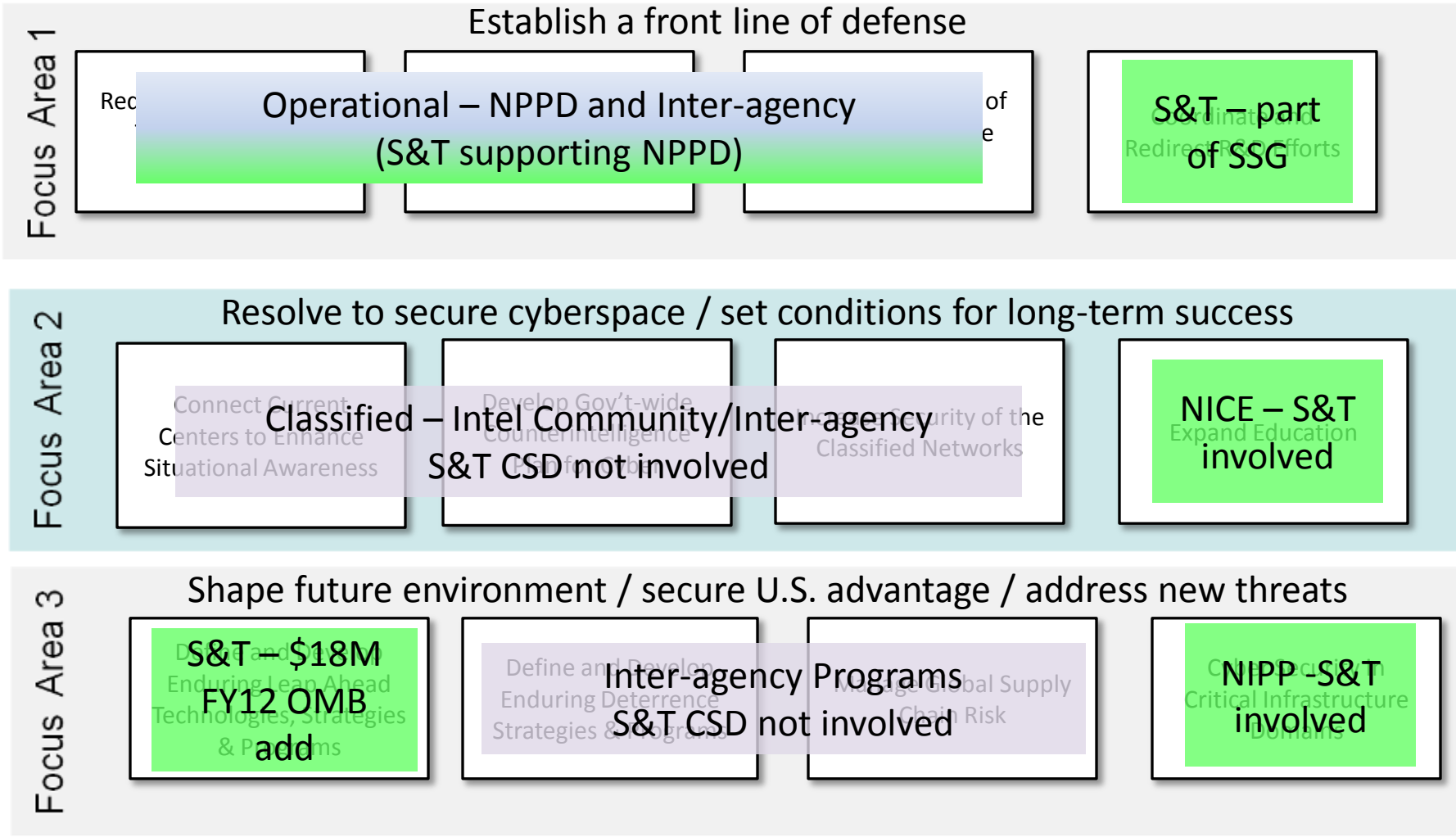
1. Preventing terrorism & enhancing security
2. Securing and managing our borders
3. Enforcing & administering immigration laws
4. Safeguarding and securing cyberspace
5. Ensuring resilience to disasters

Operational Directives

HSPD-5 National Incident Management System (2003) → HSPD-9 Defense of U.S. Agriculture & Food (2004) → HSPD-10 Biodefense for the 21st Century (2004) → HSPD-22 Domestic Chemical Defense (2007) → PPD-8 National Preparedness (2011)

Prevention, Protection, Mitigation, Response, Recovery

Comprehensive National Cybersecurity Initiative (CNCI)

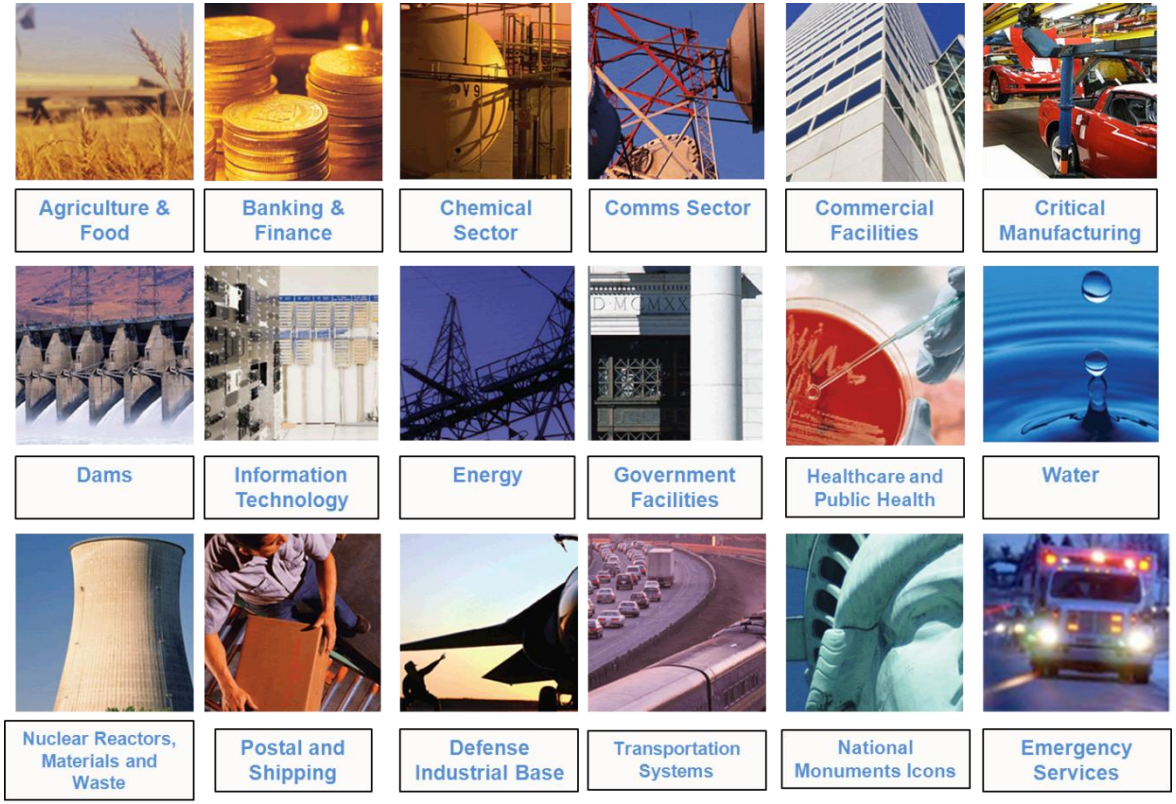


http://cybersecurity.whitehouse.gov

Homeland Security
Science and Technology

Cybersecurity for the 18 Critical Infrastructure Sectors

DHS provides advice and alerts to the 18 critical infrastructure areas …



… DHS collaborates with DoD in piloting cybersecurity for the Defense Industrial Base

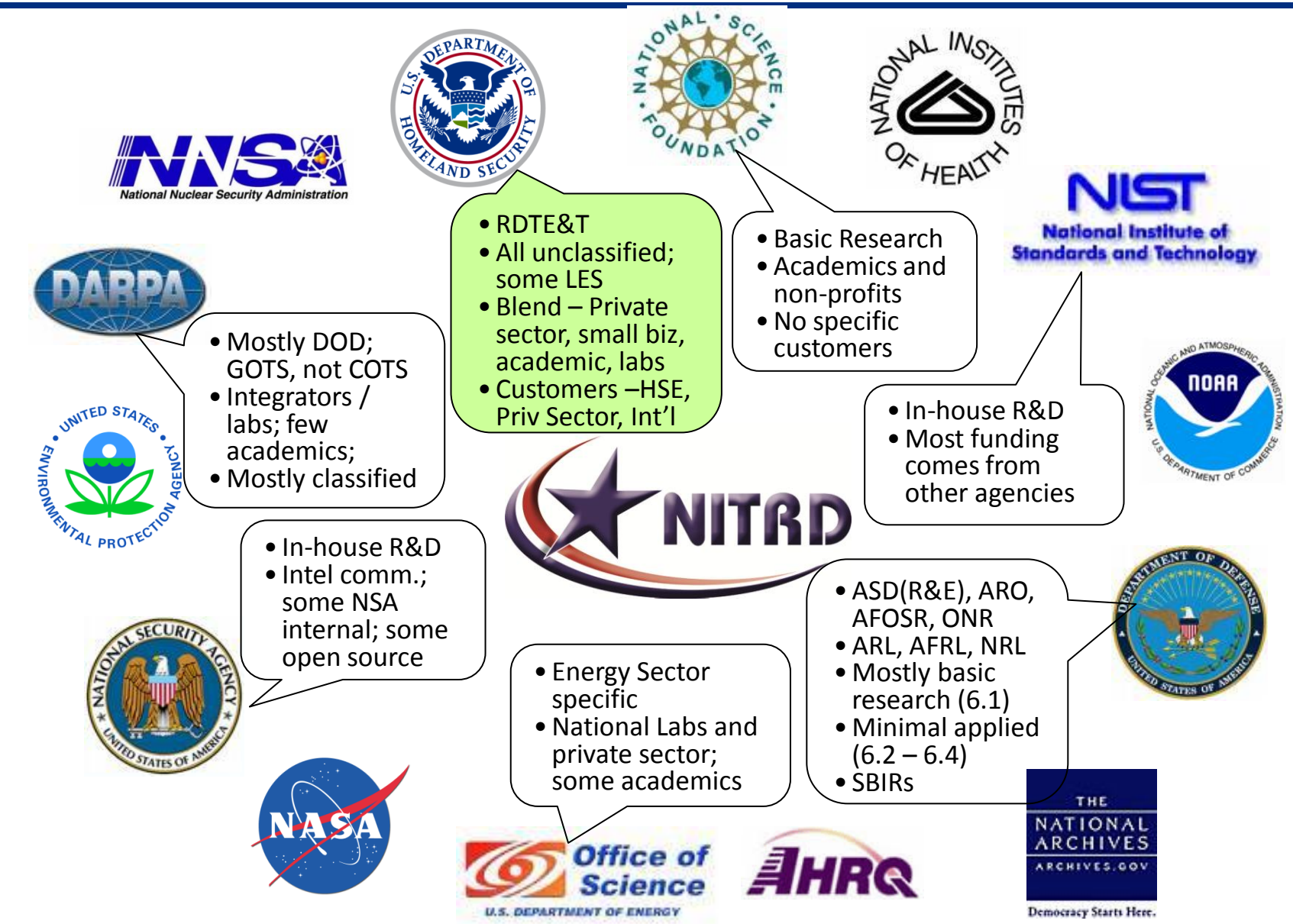
In the future, DHS will provide cybersecurity for …

- ❑ 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 …

Homeland Security
Science and Technology

NITRD Organization Roles



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

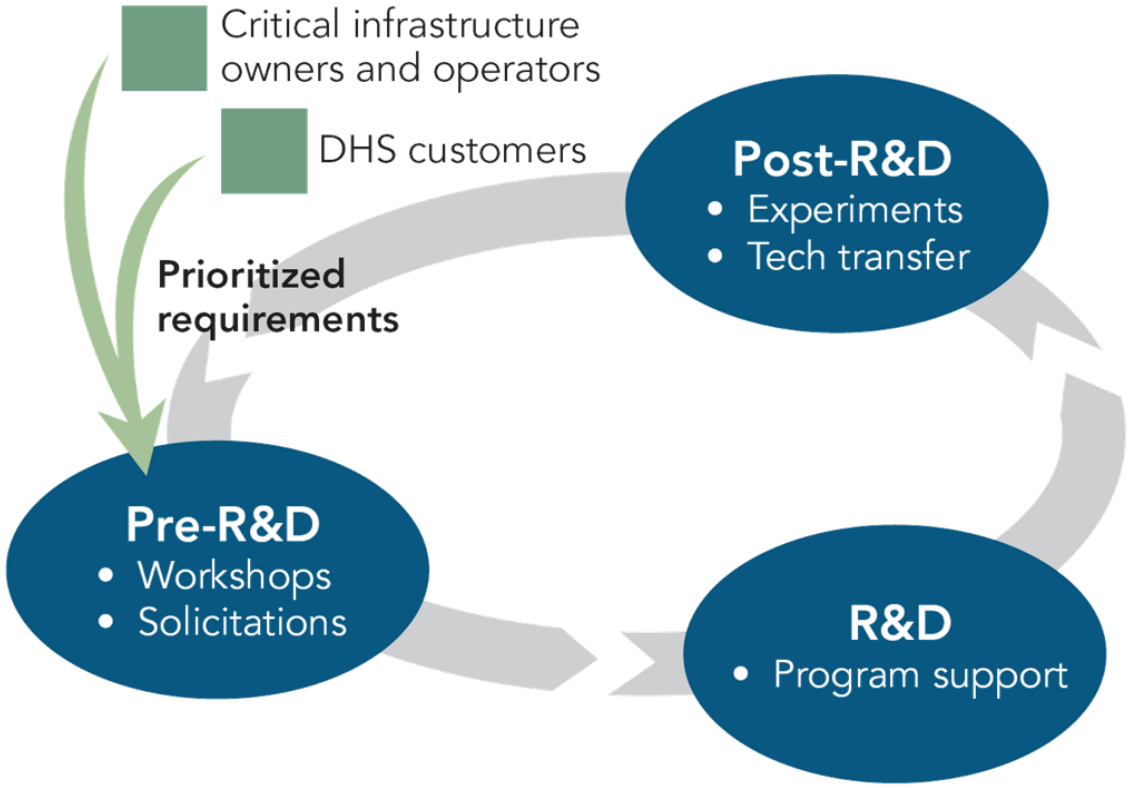
Strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise

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

Homeland Security
Science and Technology

CSD R&D Execution Model



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

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)

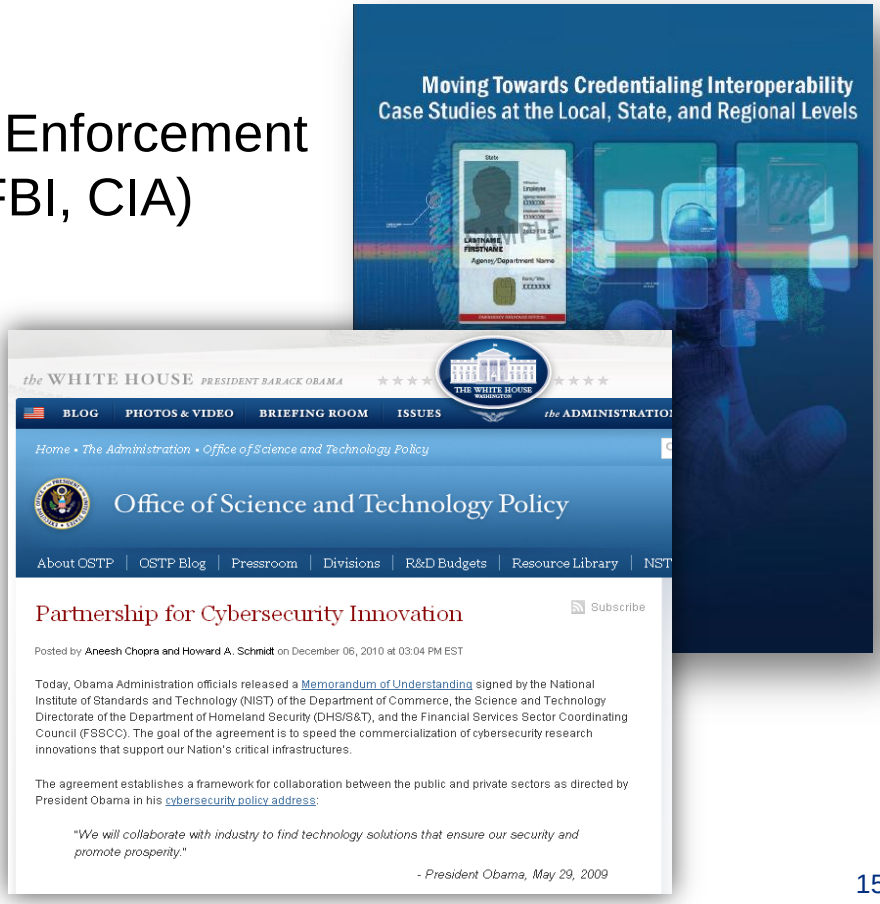
- Enterprise Level Security Metrics and Usability
- Homeland Open Security Technology (HOST)
- Software Quality Assurance
  - S2ERC – Security and Software Engineering Research Center
- Cyber Economic Incentives (CNCI)
  - New FY12 Initiative
- Leap Ahead Technologies (CNCI)
- Moving Target Defense (CNCI)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

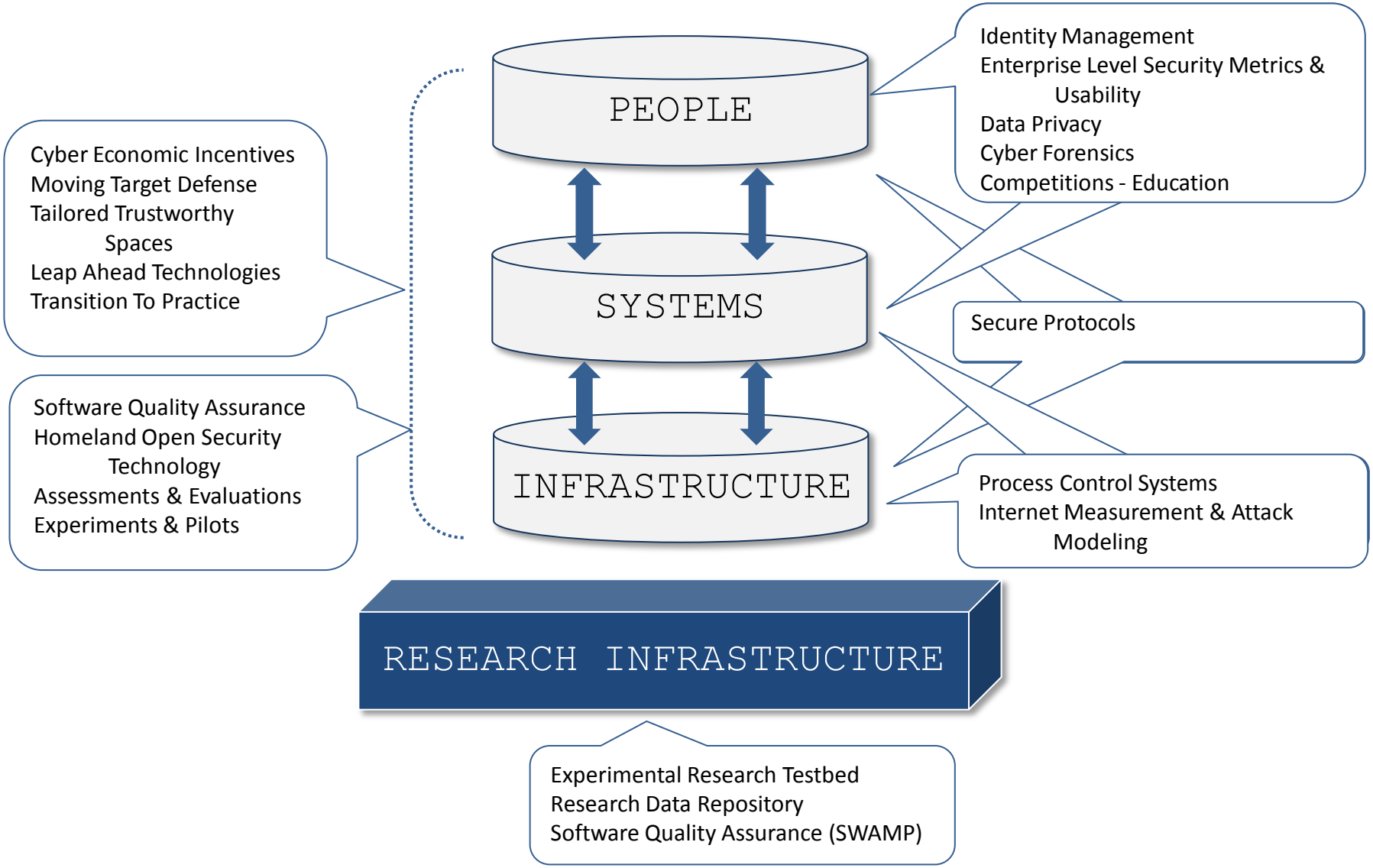
Evaluation and Transition (CTET)

- 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

Homeland Security

Science and Technology

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)	Type II (Prototype Technologies)	Type III (Mature Technologies)
✓ Applied Research Phase	✓ More Mature Prototypes	✓ Mature Technology
✓ Development Phase	✓ Development Phase	✓ Demo Only in Op Environ.
✓ Demo in Op Environ.	✓ Demo in Op Environ.	✓ Funding ≤ $750K & 12 mos.
✓ Funding ≤ $3M & 36 mos.	✓ Funding ≤ $2M & 24 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)

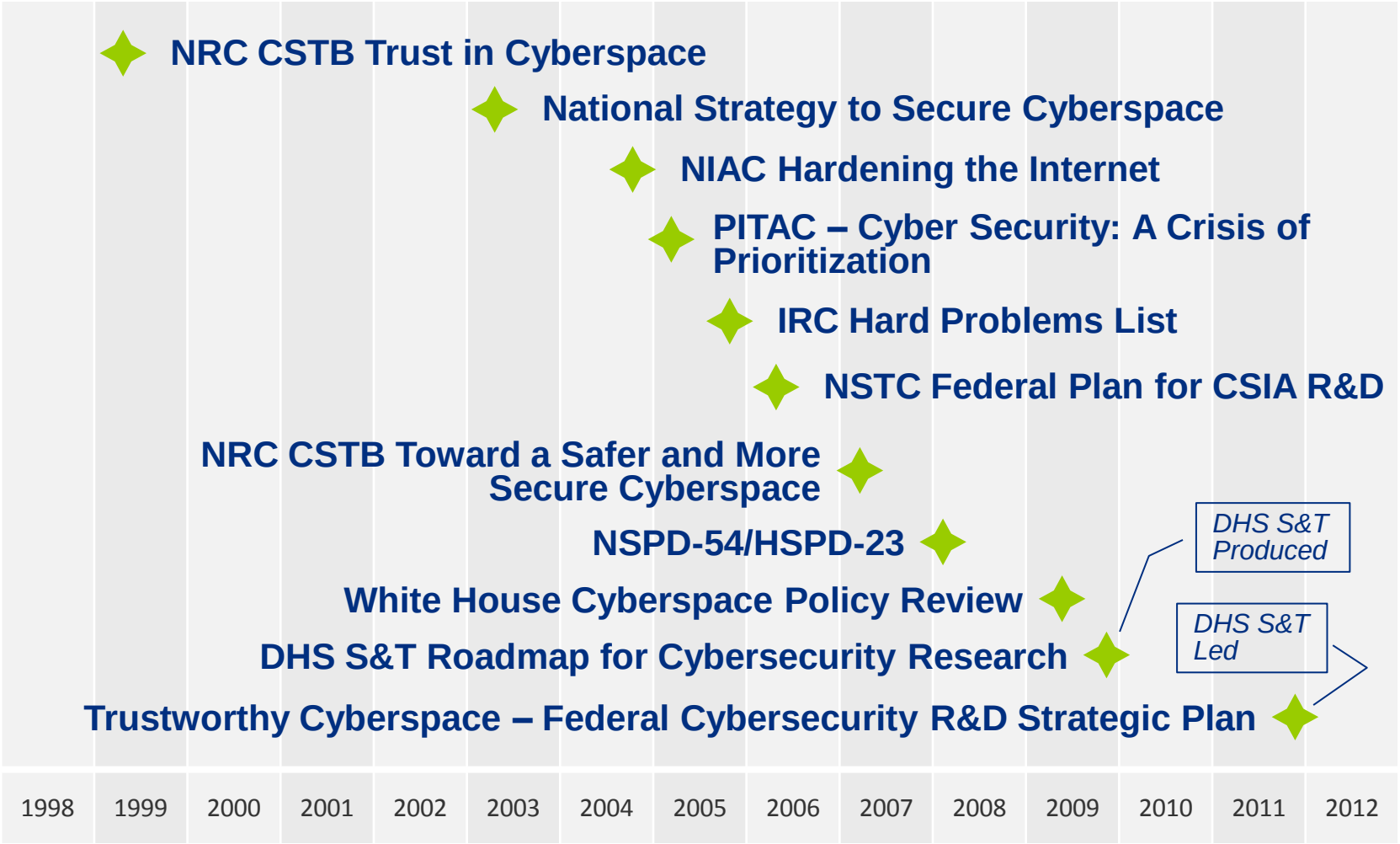
TTA-1	Software Assurance	DHS, FSSCC
TTA-2	Enterprise-Level Security Metrics	DHS, FSSCC
TTA-3	Usable Security	DHS, FSSCC
TTA-4	Insider Threat	DHS, FSSCC
TTA-5	Resilient Systems and Networks	DHS, FSSCC
TTA-6	Modeling of Internet Attacks	DHS
TTA-7	Network Mapping and Measurement	DHS
TTA-8	Incident Response 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

History of National Cyber Security Work



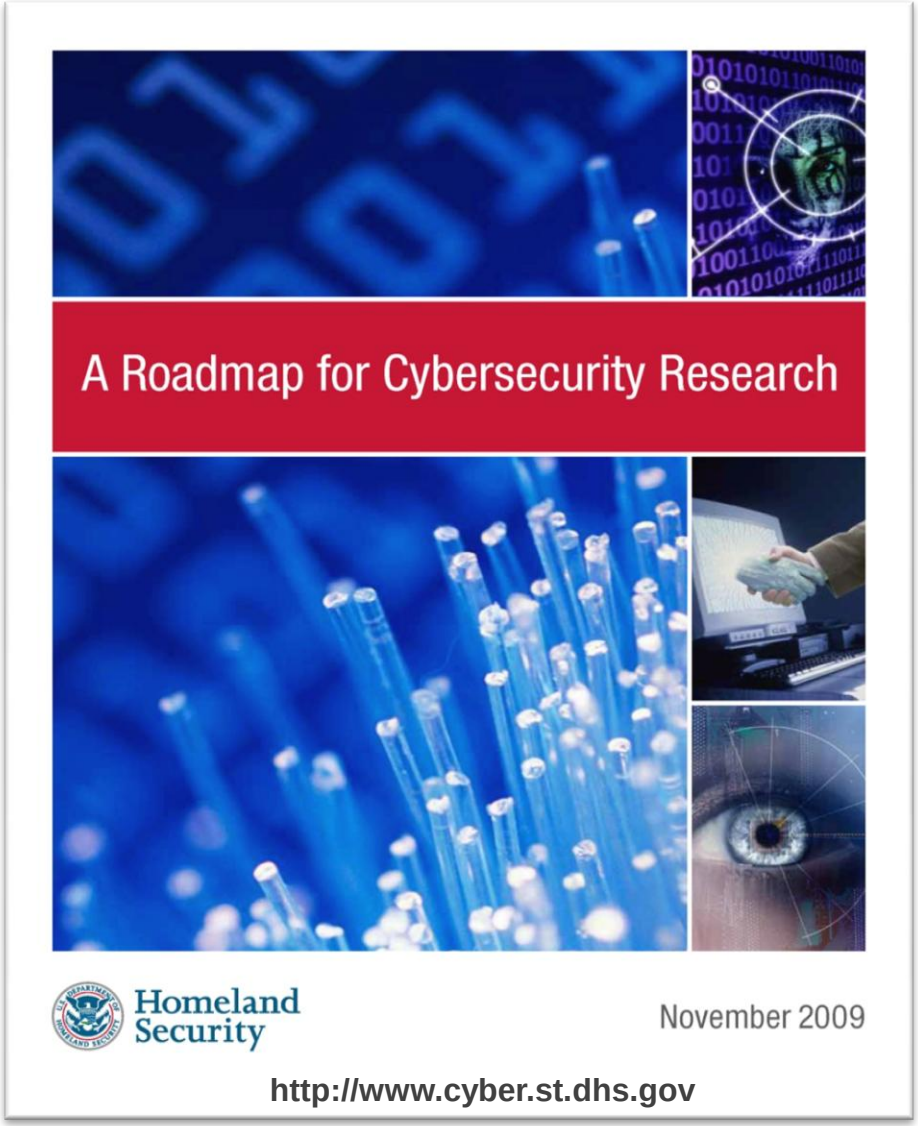
Homeland Security
Science and Technology

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

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) (Solicitation #:DHSS-TLRBAA12-07)

Homeland Security
Science and Technology

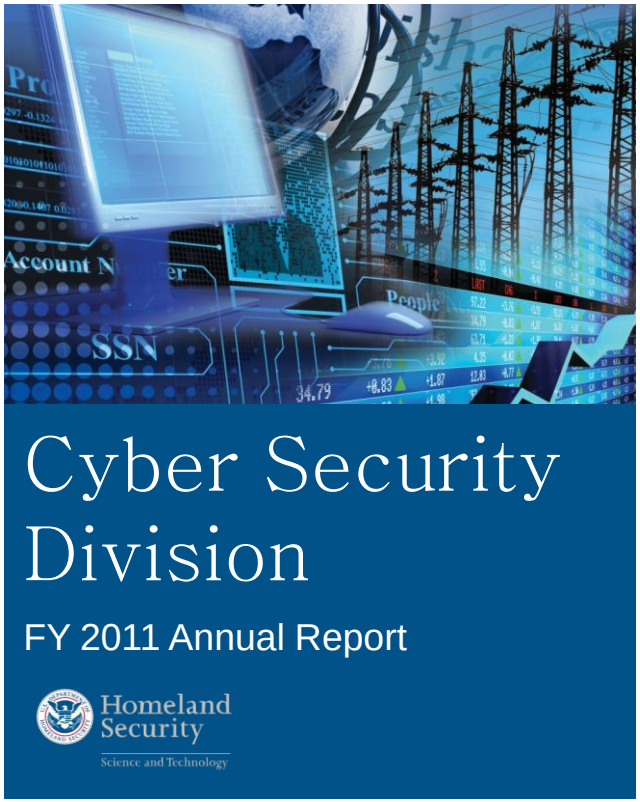
LRBAA Summary Listing

- **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.

Homeland Security
Science and Technology

Homeland Security
Science and Technology

Annual Report and Research Topics



Available NOW!

- Security in Cloud-based Systems
- Data Privacy
- Mobile and Wireless Security
- (Big) Data Analytics for Cyber Security Applications
- Embedded Device Security (e.g., CPS, medical, vehicle)
- Network Attribution / Traceback
- System Composition
- Cyber Forensics
- Cyber Education / Curriculum
- NPPD Requirements

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

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