

DHS S&T Cyber Security Division (CSD) Overview

NDIA Executive Briefing
Crystal City, VA
February 17, 2011



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



Homeland
Security

2004-2010 S&T Mission



Conduct, stimulate, and enable **research, development, test, evaluation and timely transition** of homeland security capabilities to federal, state and local operational end-users.



Homeland
Security

DHS S&T Mission

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



S&T Goals

Goal 1: Rapidly develop and deliver knowledge, analyses, and innovative solutions that advance the mission of the Department

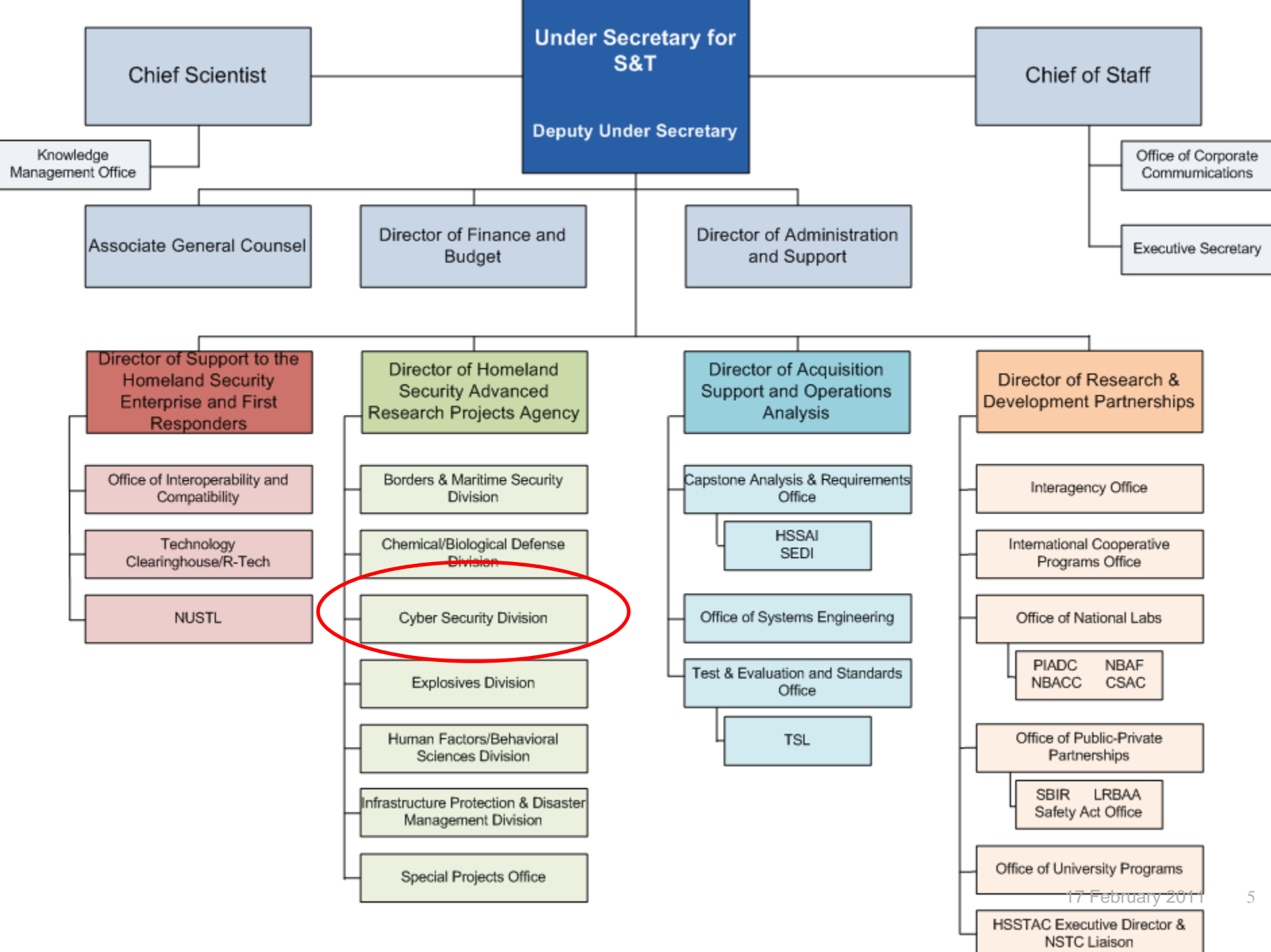
Goal 2: Leverage technical expertise to assist DHS components' efforts to establish operational requirements, and select and acquire needed technologies

Goal 3: Strengthen the Homeland Security Enterprise and First Responders' capabilities to protect the homeland and respond to disasters

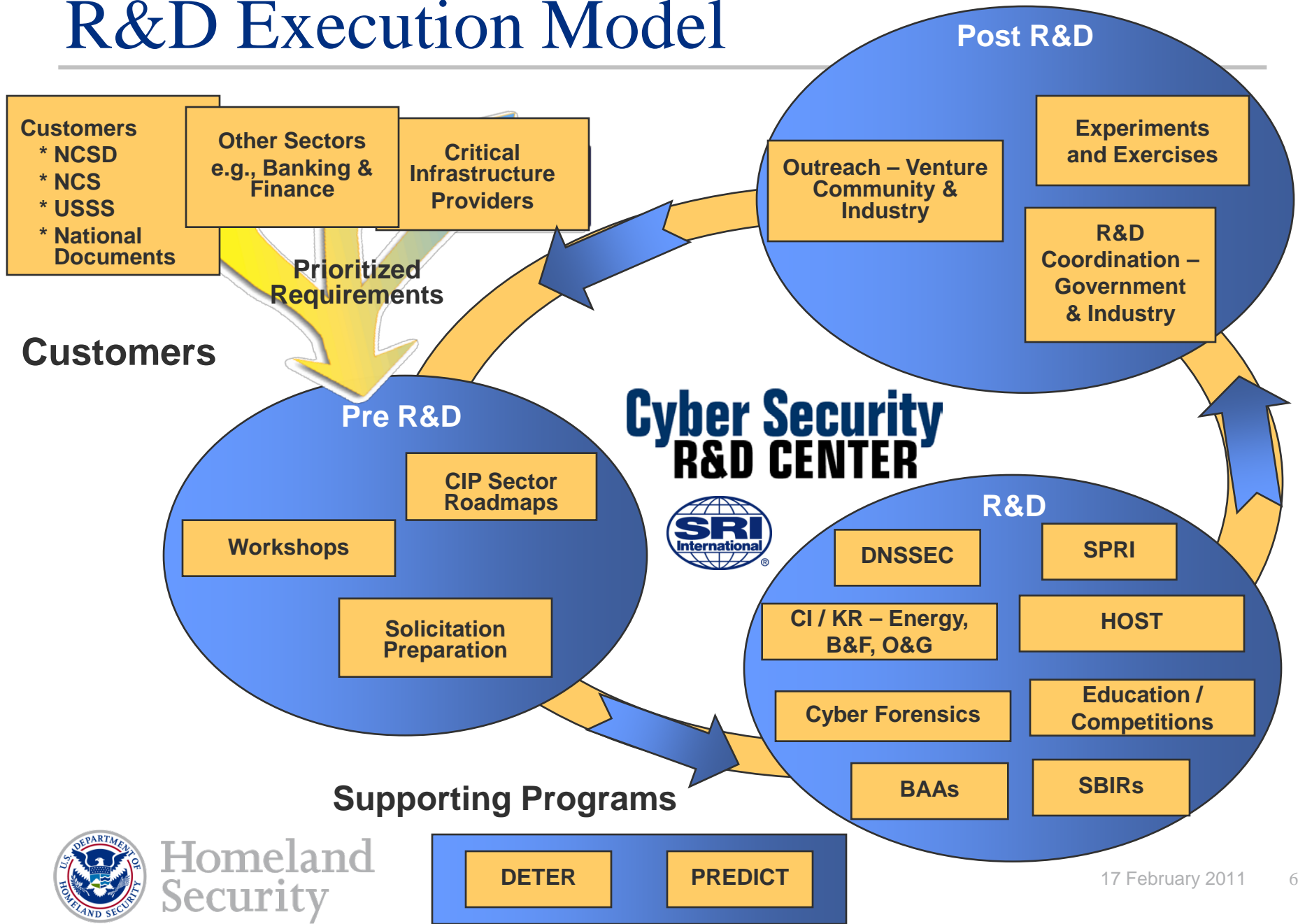
Goal 4: Conduct, catalyze, and survey scientific discoveries and inventions relevant to existing and emerging homeland security challenges

Goal 5: Foster a culture of innovation and learning, in S&T and across DHS, that addresses challenges with scientific, analytic, and technical rigor





R&D Execution Model



Homeland Security

Sample Product List

- 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 (later)
- USURF – Cyber Exercise Planning tool
 - ◆ Recently used in MA & WA state cyber exercises
- Secure64 – DNSSEC Automation
 - ◆ Several commercial customers; Government pilots underway
- HBGary – Memory and Malware Analysis
 - ◆ 12-15 pilot deployments as part of Cyber Forensics program



Sample Product List - 2

- Grammatech – Binary Analysis tools
 - ◆ Used by several Intel agencies; commercially available
- Telcordia – Automated Vulnerability Analysis
 - ◆ In use by DOD, SEC
- GMU – 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 in progress



Cyber Security Program Areas

- Internet Infrastructure Security
- Critical Infrastructure / Key Resources (CI/KR)
- National Research Infrastructure
- Cyber Forensics
- Homeland Open Security Technology (HOST)
- Identity Management / Data Privacy
- Internet Measurement and Attack Modeling
- Software Assurance - Tools and Infrastructure
- Next Generation Technologies
- Exp Deployments, Outreach, Education/Competitions
- Comp. National Cybersecurity Initiative (CNCI)
- Small Business Innovative Research (SBIR)



Internet Infrastructure Security

- DNSSEC – Domain Name System Security
 - ◆ Working with OMB, GSA, NIST to ensure USG is leading the global deployment efforts
 - <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf>
 - ◆ Working with vendor community to ensure solutions
 - <http://www.govsecinfo.com/the-keys-to-deploying-dnssec.html>
- SPRI – Secure Protocols for Routing Infrastructure
 - ◆ Working with global registries to deploy Public Key Infrastructure (PKI) between ICANN/IANA and registry and between registry and ISPs/customers
 - ◆ Working with industry to develop solutions for our current routing security problems and future technologies



Critical Infrastructure / Key Resources - 1

- LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity
 - ◆ A collaboration of oil and natural gas companies and DHS S&T to facilitate cooperative research, development, testing, and evaluation procedures to improve cyber security in Industrial Automation and Control Systems
 - Consortium under the Automation Federation
- TCIPG – Trustworthy Computing Infrastructure for the Power Grid
 - ◆ Partnership with DOE funded at UIUC with several partner universities and industry participation
 - ◆ Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power, including new resilient “smart” power grid
- DECIDE (Distributed Environment for Critical Infrastructure Decision-making Exercises)
 - ◆ Provide a dedicated exercise capability to foster an effective, practiced business continuity effort to deal with increasingly sophisticated cyber threats
 - Enterprises initiate their own exercises, define their own scenarios, protect their proprietary data, and learn vital lessons to enhance business continuity
 - ◆ The Financial Services Sector Coordinating Council R&D Committee has organized a user-group of subject matter experts paid by their respective financial institutions to support the project over the next two years.



Critical Infrastructure / Key Resources - 2



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 | NSTP

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

Financial services—banking and credit card transactions, insurance, trading and funds management, and many other business and consumer financial activities—are increasingly provided online. These services are essential in the daily lives of citizens, critical for the fast-paced conduct of modern business, and required for the healthy pulse of eCommerce, locally to globally. As a result, threats to these services are threats to individuals, companies, and the Nation. Ensuring these online services are reliable, accurate, safe, and secure against threats is a shared responsibility of the public and private sectors alike. Many of the innovations emerging from the partnership will extend beyond financial services to online health services, the Smart Grid, and the Nation's water, transportation, and other critical infrastructures.

This agreement will accelerate the deployment of network testbeds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures' functions, processes, and people by:

1. Facilitating coordination and cooperation among Federal agencies and the financial services sector in the development and delivery of innovative cybersecurity technologies and processes; and
2. Establishing clear processes for the implementation of specific use cases.

- MOU between DHS S&T, NIST, and FS Sector Coord Council (FSSCC) in coordination with WH
- Framework for public-private collaboration on R&D projects for the FS
- Initial projects
 - ◆ High Assurance Domains (e.g., DNSSEC)
 - ◆ Identity Management

National Research Infrastructure

- DETER - <http://www.isi.edu/deter/>
 - ◆ Researcher and vendor-neutral experimental infrastructure that is open to a wide community of users to support the development and demonstration of next-generation cyber defense technologies
 - ◆ Over 170 users from 14 countries (and growing)
- PREDICT – <https://www.predict.org>
 - ◆ Repository of network data for use by the U.S.- based cyber security research community
 - ◆ Privacy Impact Assessment (PIA) completed
 - ◆ Over 140 datasets and growing; Over 100 active users (and growing)

**End Goal: Improve the quality of defensive
cyber security technologies**



Cyber Forensics

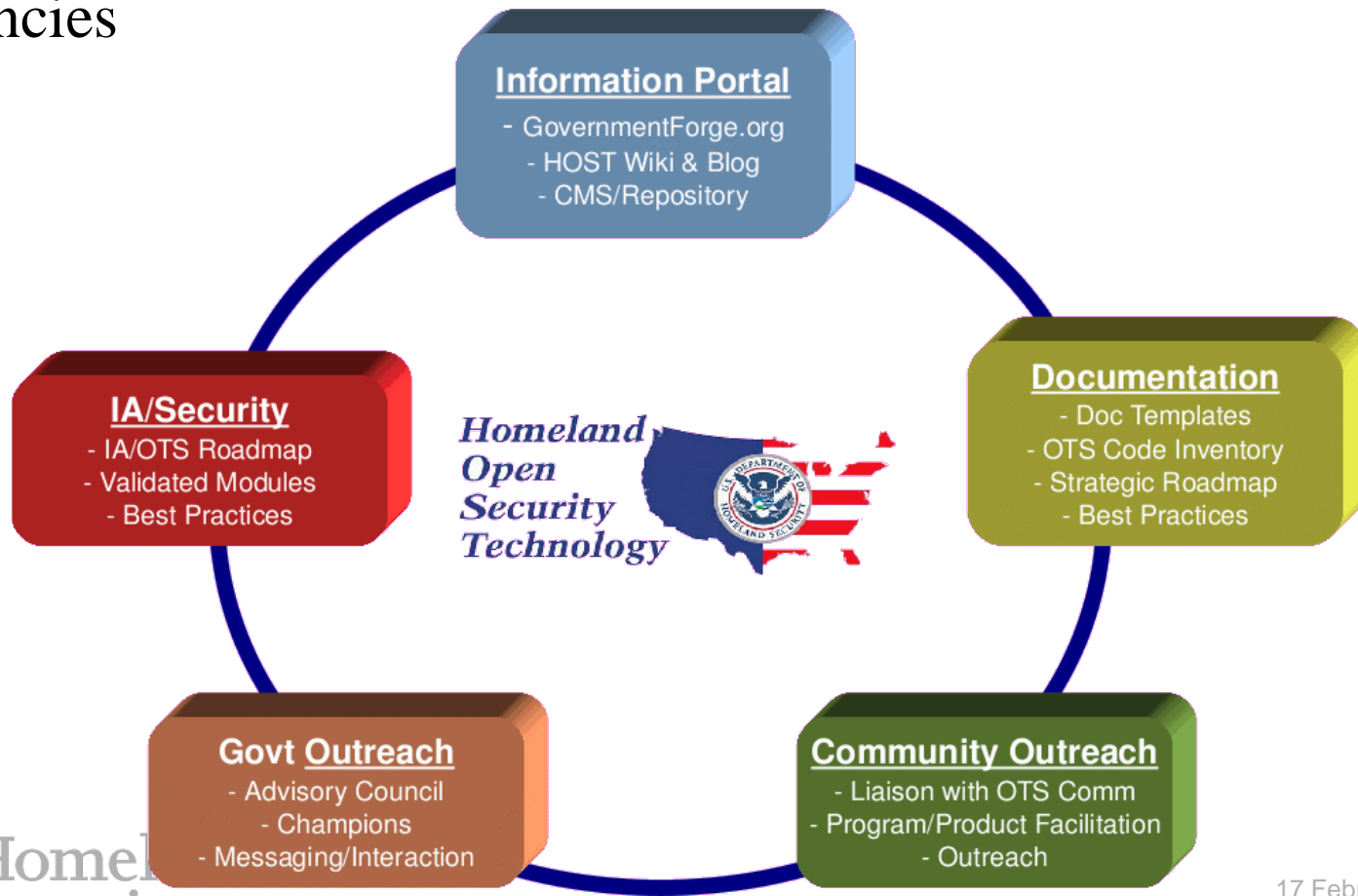
- Initial requirements working group held Nov 2008; second meeting held Oct 2010
 - ◆ Attendees from USSS, CBP, ICE, FLETC, FBI, NIJ, NIST
- Initial list of projects
 - ◆ Mobile device forensic tools
 - ◆ GPS forensics tools
 - ◆ LE First responder “field analysis kit”
 - ◆ High-speed data capture and deep packet inspection
 - ◆ Live stream capture for gaming systems
 - ◆ Memory analysis and malware tools
 - ◆ Information Clearing House
- S&T initiated 6 projects in FY09; More in FY11

} Combined



Homeland Open Security Technology (HOST)

- Promote the development and implementation of open source solutions within US Federal, state and municipal government agencies



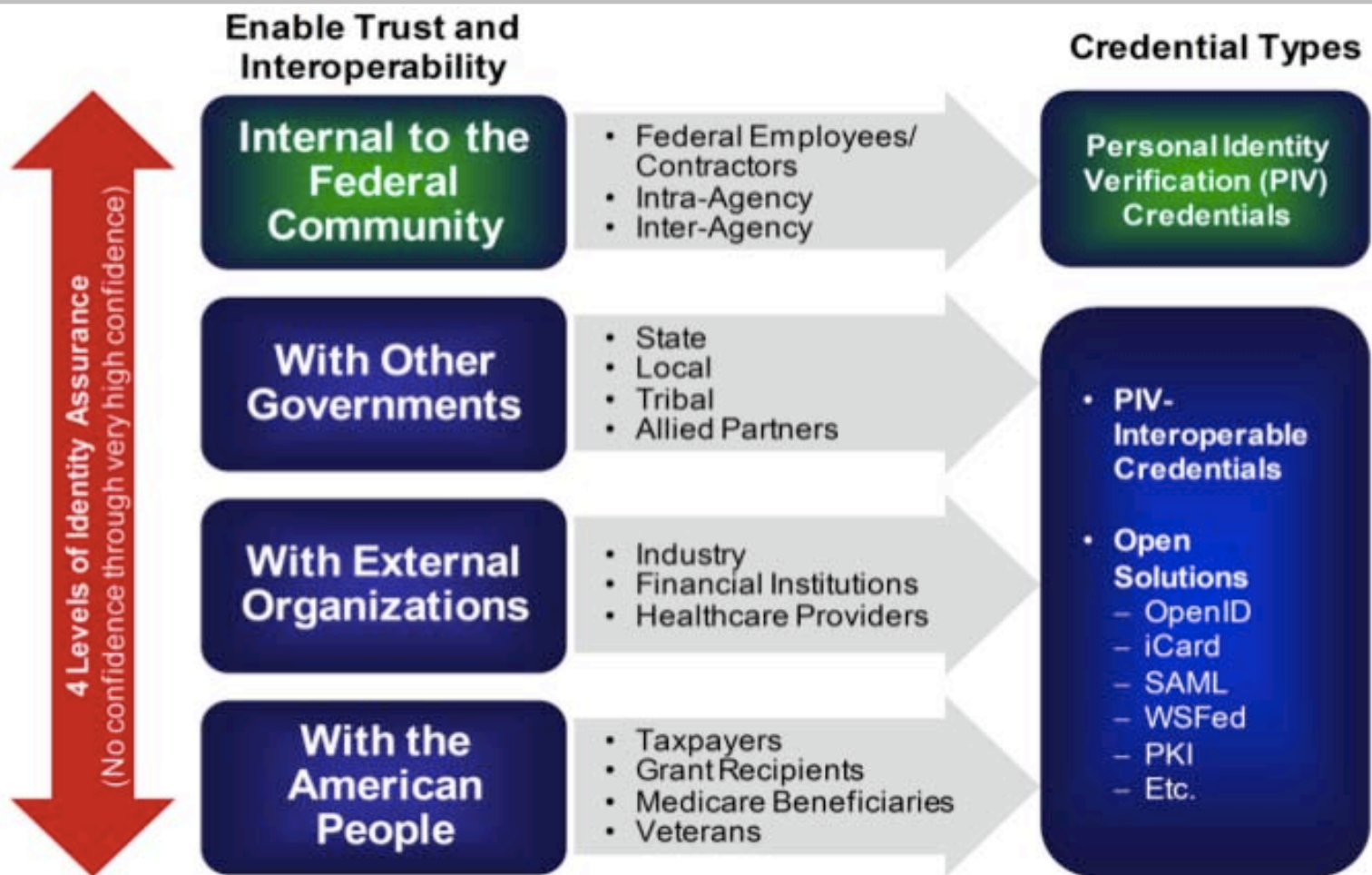
Homeland
Security

HOST Program Areas

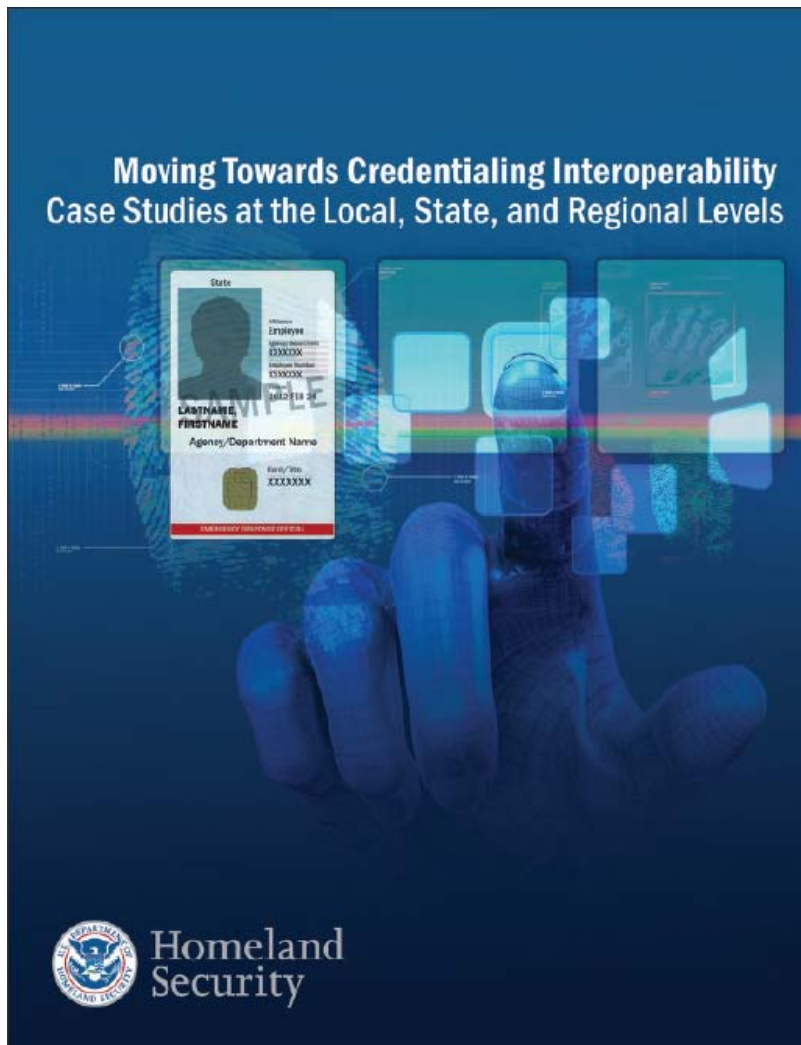
- Information Portal
 - ◆ Federal Government Open Source Census
 - ◆ GovernmentForge Open Source Software Repository
- Documentation
 - ◆ Standards, Best Practices
- Community Outreach
 - ◆ “New” open source IDS/IPS – OISF and Suricata
- Information Assurance / Security
 - ◆ US Government security evaluation processes (OpenSSL)
- S&T initiated HOST in FY09/10



Identity Management



Case Study



- **Case Study Report**

- Published on www.safecomprogram.gov

- **Credentialing Challenges**

- Multiple stove-piped credentials
- Multi-jurisdictional response to large-scale disasters
- Lack of trust and interoperability
- Too many credentials!
- Insecure physical and logical access

Internet Measurement / Attack Modeling

- Technologies for the protection of key infrastructure via development of, and integration between, reliable capabilities such as:
 - ◆ Geographic mapping of Internet resources, (e.g., IPV4 or IPV6 addresses, hosts, routers, DNS servers, either wired or wireless), to GPS-compatible locations (latitude/longitude).
 - ◆ Logically and/or physically connected maps of Internet resources (IP addresses, hosts, routers, DNS servers and possibly other wired or wireless devices).
 - ◆ Detailed maps depicting ISP peering relationships, and matching IP address interfaces to physical routers.

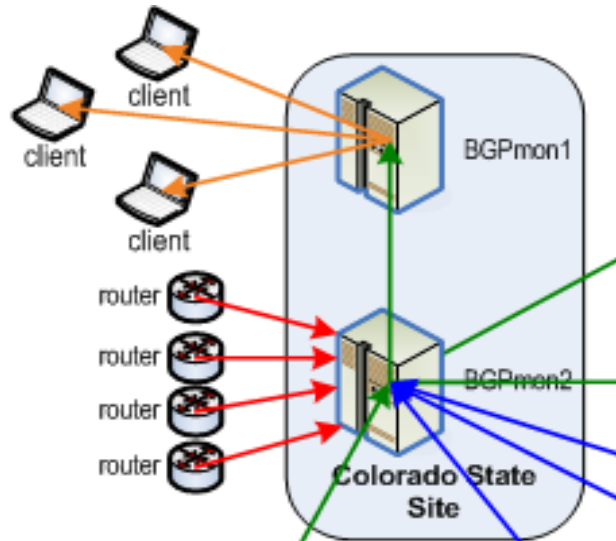


Internet Measurement / Attack Modeling

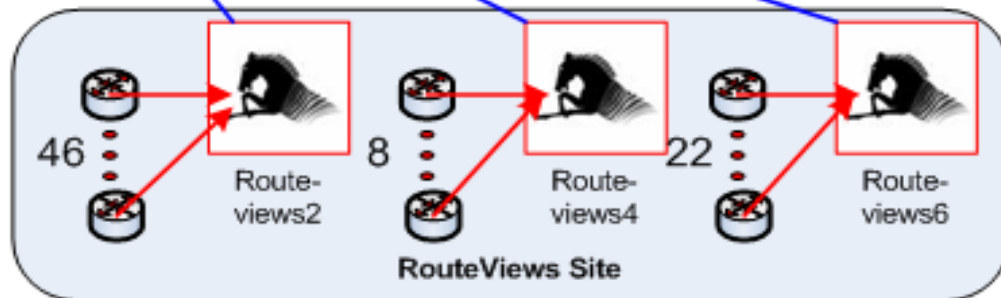
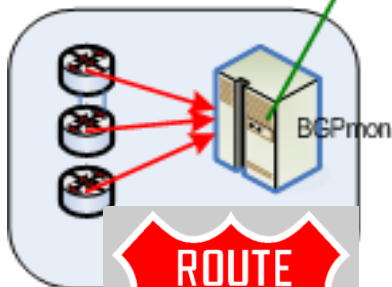
- ◆ Monitoring and archiving of BGP route information.
- ◆ Development of systems achieving improvement to the security and resiliency of our nation's cyber infrastructure.
- ◆ Monitoring and measurement applied to detection and mitigation of attacks on routing infrastructure, and supporting the development and deployment of secure routing protocols.
- ◆ Monitoring and measurement contributing to understanding of Domain Naming System (DNS) behavior, both in terms of its changing role in distributed Internet scale malware activities, such as botnets, and DNS's behavior as a system under change through DNSSEC and other potential changes affecting the root level.



RouteViews Data in Real-Time



- You can receive updates and routing tables in real-time
- Updates: **129.82.138.26 TCP port 50001**
- Tables: **129.82.138.26 TCP port 50002**
- <http://bgpmon.netsec.colostate.edu>



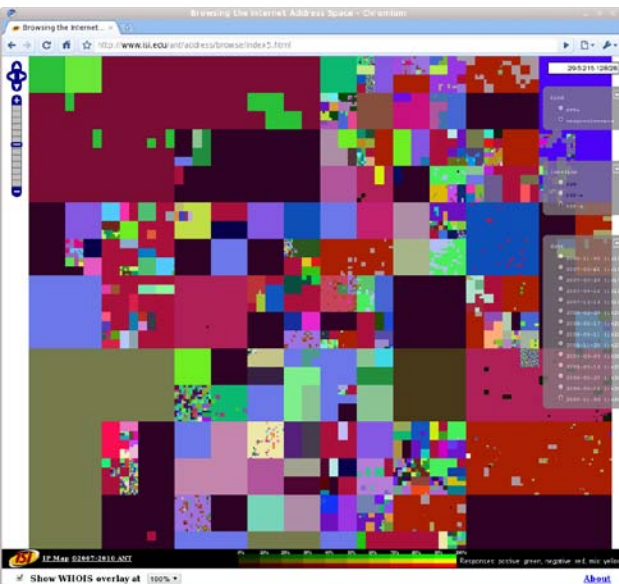
Security

AMITE: New Results and Conclusions

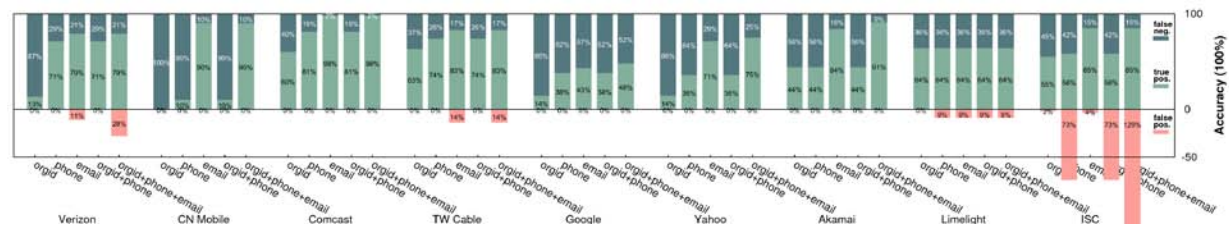
IP hitlist evaluation



address visualization improvements



AS-to-org. mapping



<http://www.isi.edu/ant/>



Homeland Security

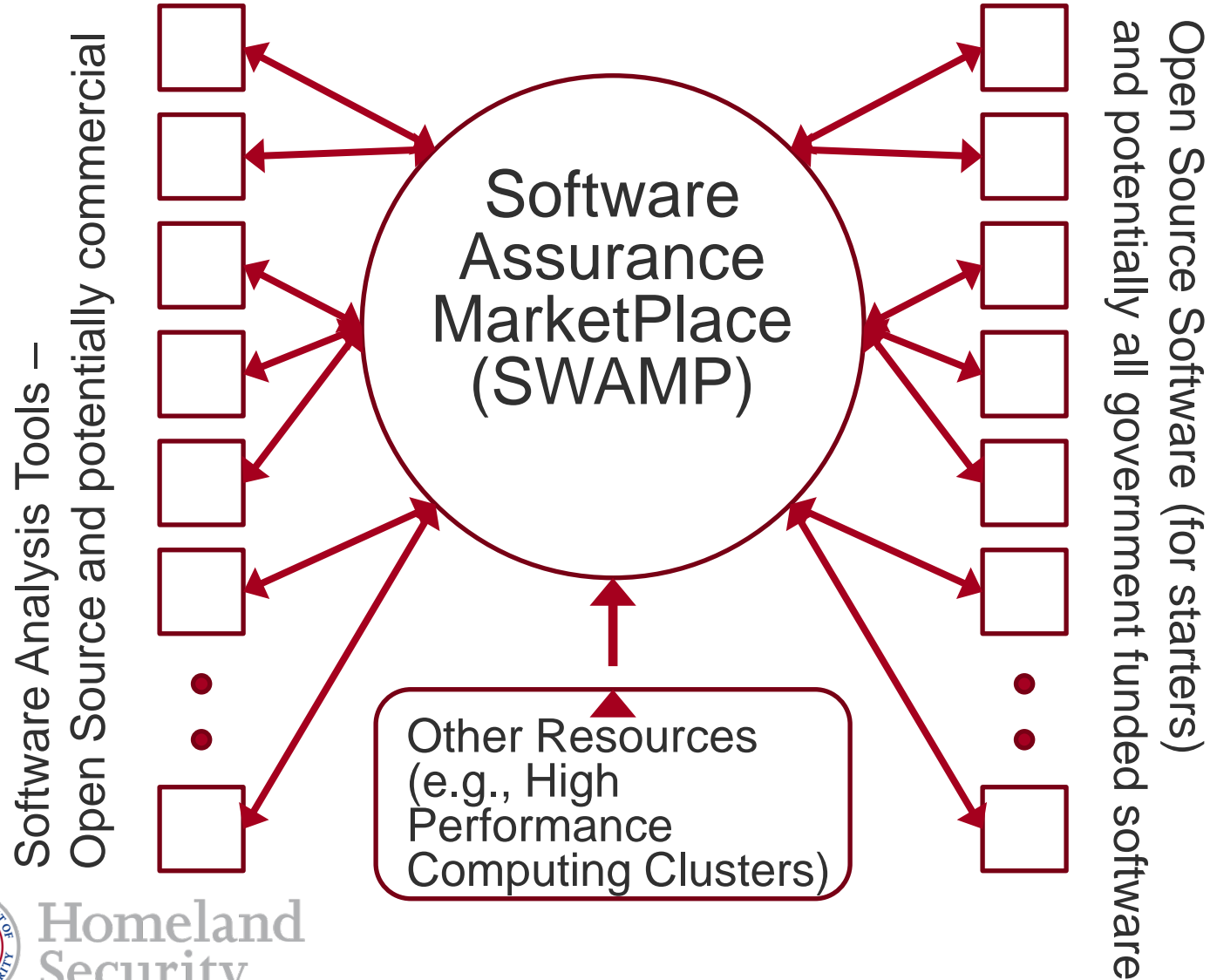
Software Assurance – SBIR Phase I Awards

- See <https://www.sbir.dhs.gov/Awards.asp> for abstracts
- “Software Assurance Analysis and Visual Analytics” – **Applied Visions, Inc. (NY)**
- “Eliminating barriers to code quality and security with increased timeliness and accuracy of analysis” – **Coverity, Inc. (CA)**
- “Run Time Tools Output Integration Framework” – **Data Access Technologies, Inc. (VA)**
- “Concolic Testing with Metronome” – **Grammatech, Inc. (NY)**
- “CodeSonar with Metronome” – **Grammatech, Inc. (NY)**
- “Concurrency vulnerabilities: Combining dynamic and static analyses for detection and remediation” – **SureLogic, Inc. (PA)**
- “Virtualization and Static Analysis to Detect Memory Overwriting Vulnerabilities” – **Zephyr Software, LLC (VA)**



- Give open source community access to entire toolset
 - ◆ Open-source developers register their project.
Coverity automatically downloads and runs tool over it.
 - ◆ Developers get back bugs in coverity's bug database
- Big success:
 - ◆ Roughly 500 projects registered
 - ◆ 4,700+ defects actually patched.
 - ◆ Some really crucial bugs found; dozens of security patches (e.g., X, ethereal)

SWAMP Conceptual Architecture



Next Generation Technologies

- <https://baa2.st.dhs.gov>
- R&D funding model that 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.
 - ◆ To perform research and development (R&D) aimed at **improving the security of existing deployed technologies** and to ensure the security of new emerging systems;
 - ◆ To **facilitate the transfer of these technologies** into the national infrastructure as a matter of urgency.
- TTAs 2, 3, 4, 5, and 8



Experimental Deployments

- **NCSA / US-CERT**

- ◆ Botnet Detection and Mitigation technology from Univ of Michigan
- ◆ Data Visualization technology from Secure Decisions (NY)

- **DHS S&T CIO**

- ◆ Secure Wireless Access Prototype from BAE Systems (VA)
 - 50 user deployment within S&T; FLETC pilot; Working with CIO/CISO
- ◆ SCADA system event detection technology from Digital Bond (FL)
 - Deployment on S&T Plum Island system

- **DOD Research and Engineering Network (DREN)**

- ◆ Botnet Detection and Mitigation technology from Georgia Tech (GA) and Milcord (MA)

- **Regional Technology Integration Initiative (S&T IGD partner)**

- ◆ City of Seattle and surrounding cities
- ◆ Botnet Detection and Mitigation technology from Univ of Michigan



Outreach and Partnership Building

- **System Integrator Forum** – held twice in WDC
 - ◆ Assist DHS S&T-funded researchers in transferring technology to larger, established security technology companies
- **Information Technology Security Entrepreneurs Forum (ITSEF)** – held four times at Stanford in Palo Alto, CA
 - ◆ Partner with the venture capital community to assist entrepreneurs and small business better understand both the government marketplace and the venture community
 - Next one in March 2011; Another one in WDC in October 2011
- **Infosec Technology Transition Council (ITTC)**
 - ◆ Held tri-annually in Menlo Park, CA
 - ◆ Attendees include venture capitalists, industry, law enforcement, academia, and government

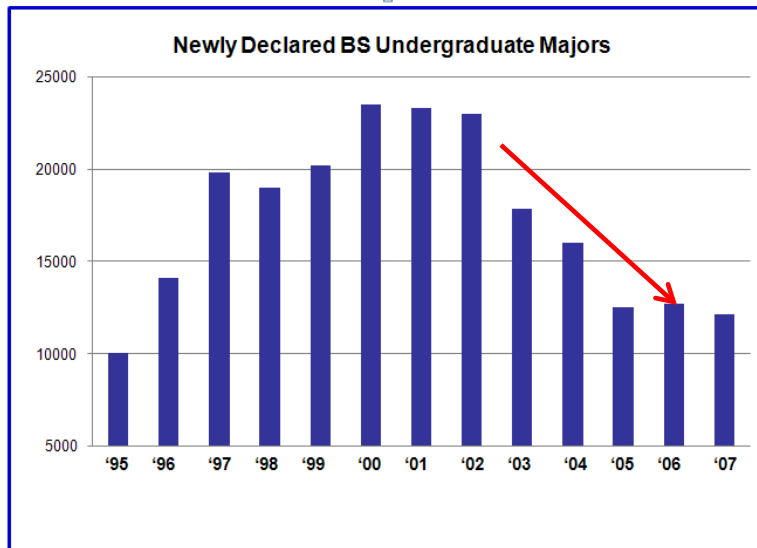


Our Education Problem

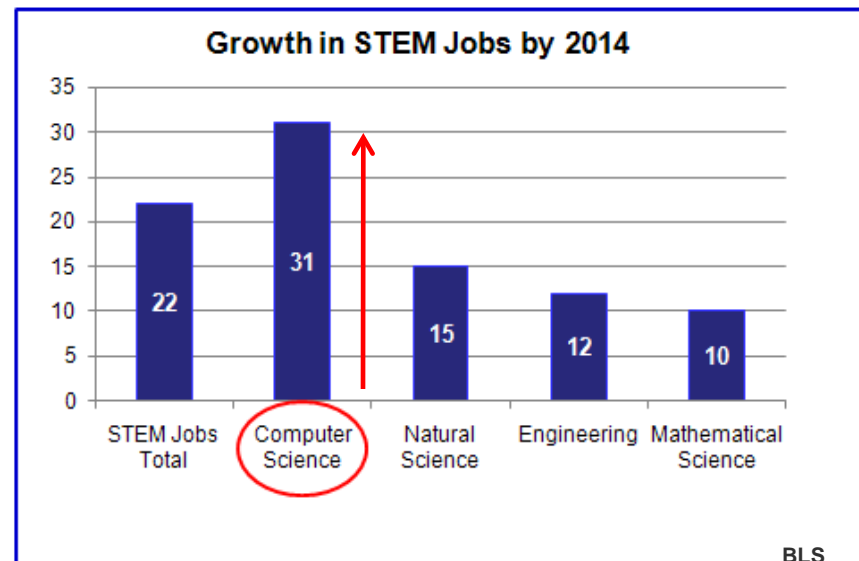


Problem: The U.S. is not producing enough computer scientists and CS degrees

- CS/CE enrollments are down 50% from 5 years ago¹
- CS jobs are growing faster than the national average²



Taulbee Survey, CRA



BLS

Computer Science/STEM have been the basis for American growth for 60 years

The gap in production of CS threatens continued growth and also national security

Defense, DHS, CNCI and industry all need more CS and CE competencies now



Homeland Security

¹Taulbee Survey 2006-2007, Computer Research Association, May 2008 Computing Research News, Vol. 20/No. 3

²Nicholas Terrell, Bureau of Labor Statistics, *STEM Occupations*, Occupational Outlook Quarterly, Spring 2007

National Initiative for Cybersecurity Education (NICE)

- National Cybersecurity Awareness (Lead: DHS).
 - ◆ Public service campaigns to promote cybersecurity and responsible use of the Internet
- Formal Cybersecurity Education (Co-Leads: DoEd and OSTP).
 - ◆ Education programs encompassing K-12, higher education, and vocational programs related to cybersecurity
- Federal Cybersecurity Workforce Structure (Lead: OPM).
 - ◆ Defining government cybersecurity jobs and skills and competencies required.
 - ◆ New strategies to ensure federal agencies attract, recruit, and retain skilled employees to accomplish cybersecurity missions.
- Cybersecurity Workforce Training and Professional Development (Tri-Leads: DoD, ODNI, DHS).
 - ◆ Cybersecurity training and professional development required for federal government civilian, military, and contractor personnel.



CCDC Mission

- The mission of the Collegiate Cyber Defense Competition (CCDC) system is to provide institutions with an information assurance or computer security curriculum 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.**
- CCDC Events are designed to:
 - ◆ Build a meaningful mechanism by which institutions of higher education may evaluate their current educational programs
 - ◆ Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work
 - ◆ Foster a spirit of teamwork, **ethical behavior**, and effective communication both within and across teams
 - ◆ Create interest and awareness among participating institutions and students



U.S. Cyber Challenge



- DC3 Digital Forensics Challenge
 - ◆ An Air Force Association national high school cyber defense competition
- CyberPatriot Defense Competition
 - ◆ A Department of Defense Cyber Crime Center competition focusing on cyber investigation and forensics
- Netwars Capture-the-Flag Competition
 - ◆ A SANS Institute challenge testing mastery of vulnerabilities



Homeland
Security

12 CNCI Projects

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

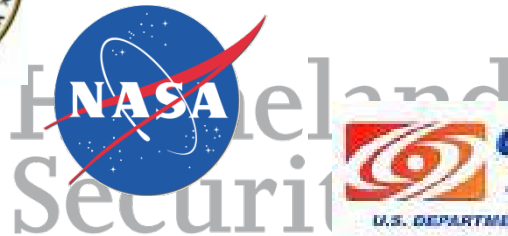
CNCI = Comprehensive National Cyber Initiative

17 February 2011

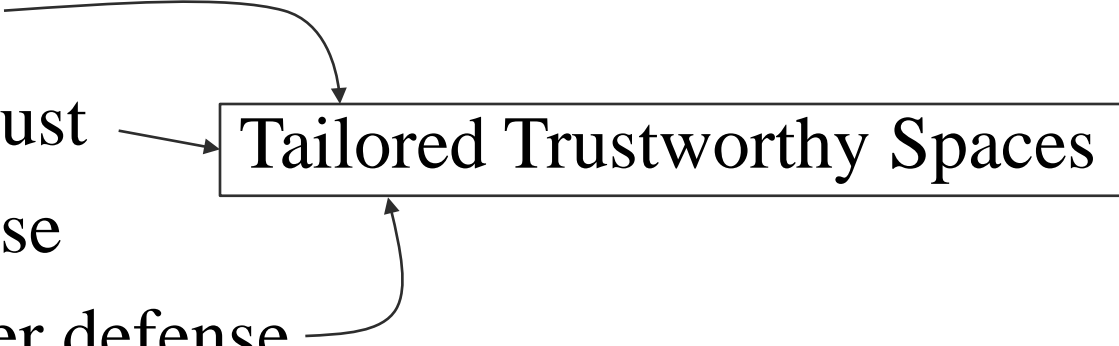
33



Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes



NCLY Summit Topics – R&D Themes

- Cyber economics
 - Digital provenance
 - Hardware enabled trust
 - Moving target defense
 - Nature-inspired cyber defense
- Tailored Trustworthy Spaces
- Expectation: Agencies will be using these topic areas in future solicitations (FY11 and beyond)
- 



Transition to Practice

- “Program” Activities
 - ◆ Technology Discovery
 - ◆ Test and Evaluation / Experimental Deployment
 - ◆ Transition / Adoption / Commercialization



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



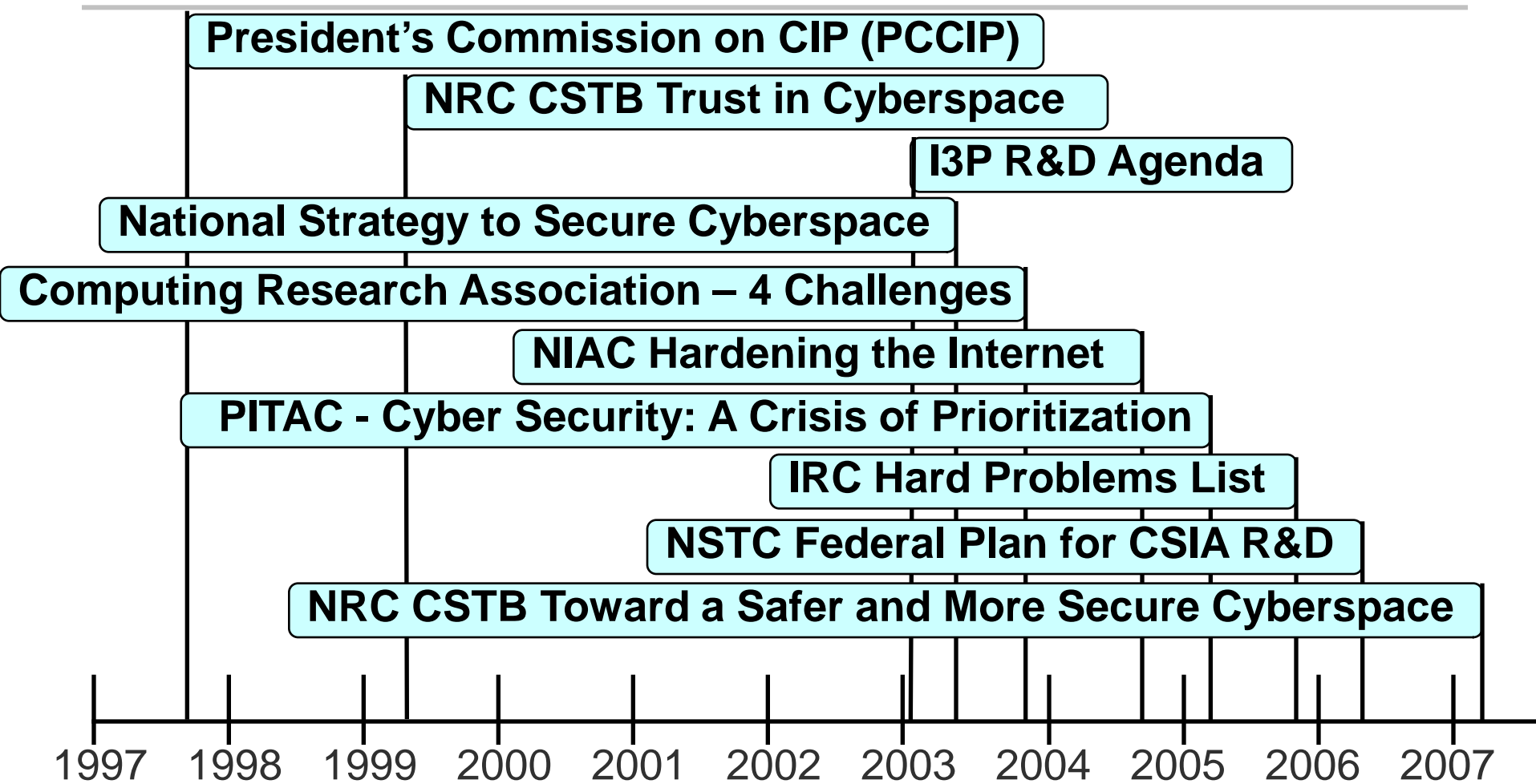
Small Business Innovative Research (SBIR)

- Important program for creating new innovation and accelerating transition into the marketplace
- Since 2004, DHS S&T Cyber Security has had:
 - ◆ 47 Phase I efforts
 - ◆ 22 Phase II efforts
 - ◆ 8 efforts currently in progress

 - ◆ 8 commercial products available
 - ◆ Three 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



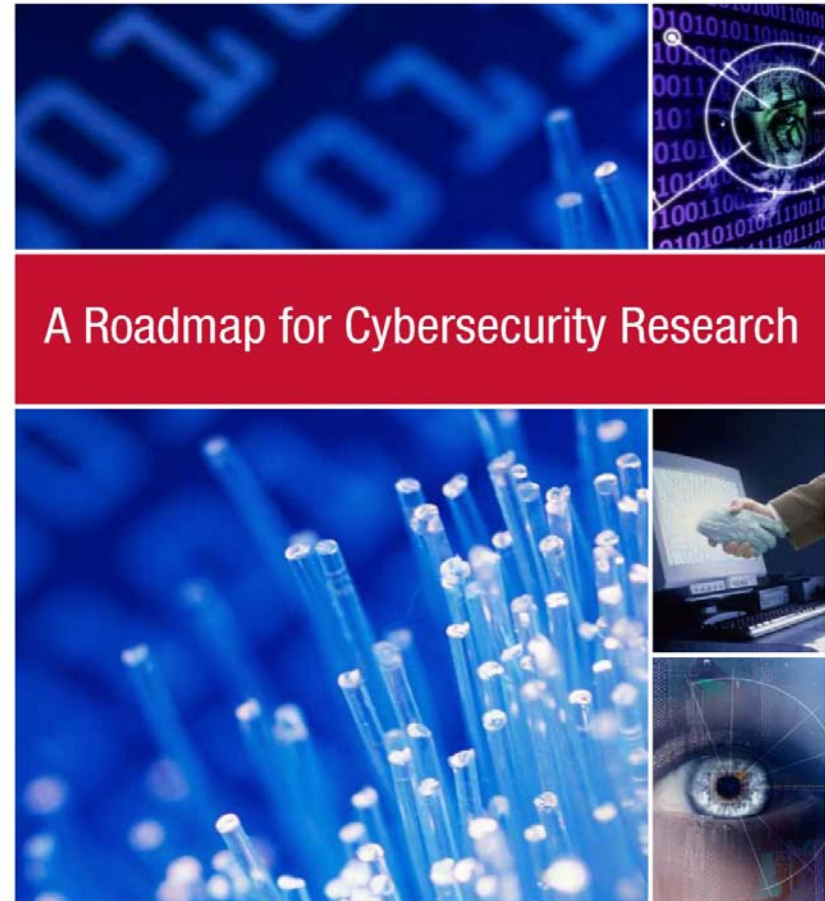
Timeline of Past Research Reports



A Roadmap for Cybersecurity Research

- ◆ <http://www.cyber.st.dhs.gov>

- ◆ Scalable Trustworthy Systems
- ◆ Enterprise Level Metrics
- ◆ System Evaluation Lifecycle
- ◆ Combatting Insider Threats
- ◆ Combatting 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

November 2009



Homeland
Security

DHS S&T Roadmap Content

- What is the problem being addressed?
- What are the potential threats?
- Who are the potential beneficiaries? What are their respective needs?
- What is the current state of practice?
- What is the status of current research?
- What are the research gaps?
- What challenges must be addressed?
- What resources are needed?
- How do we test & evaluate solutions?
- What are the measures of success?



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 *S&T*



BAA Program / Proposal Structure

- **NOTE: Deployment Phase = Test, Evaluation, and Pilot deployment in (DHS) “customer” environments**
- Type I (New Technologies)
 - ◆ New technologies with an applied research phase, a development phase, and a deployment phase (optional)
 - Funding not to exceed 36 months (including deployment phase)
- Type II (Prototype Technologies)
 - ◆ More mature prototype technologies with a development phase and a deployment phase (optional)
 - Funding not to exceed 24 months (including deployment phase)
- Type III (Mature Technologies)
 - ◆ Mature technology with a deployment phase only.
 - Funding not to exceed 12 months



DHS S&T BAA Schedule

- White Paper Registration – Feb 16, 2011
- White Papers – Due March 1, 2011
- Proposal Notification – April 12, 2011
- Full Proposals – Due May 26, 2011
- Funding Notification – July 18, 2011
- Contract Awards NLT Oct 31, 2011

- Over \$40M funded over 36 months



Summary

- DHS S&T continues with an aggressive cyber security research agenda
 - ◆ Working with the community to solve the cyber security problems of our current (and future) infrastructure
 - Outreach to communities outside of the Federal government, i.e., building public-private partnerships is essential
 - ◆ 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