Federal R&D Landscape and DHS S&T

SwA WG meeting
MITRE, McLean, VA
November 29, 2011

Edward Rhyne

Program Manager

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

edward.rhyne@dhs.gov

202-254-6121

Homeland Security
Science and Technology

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

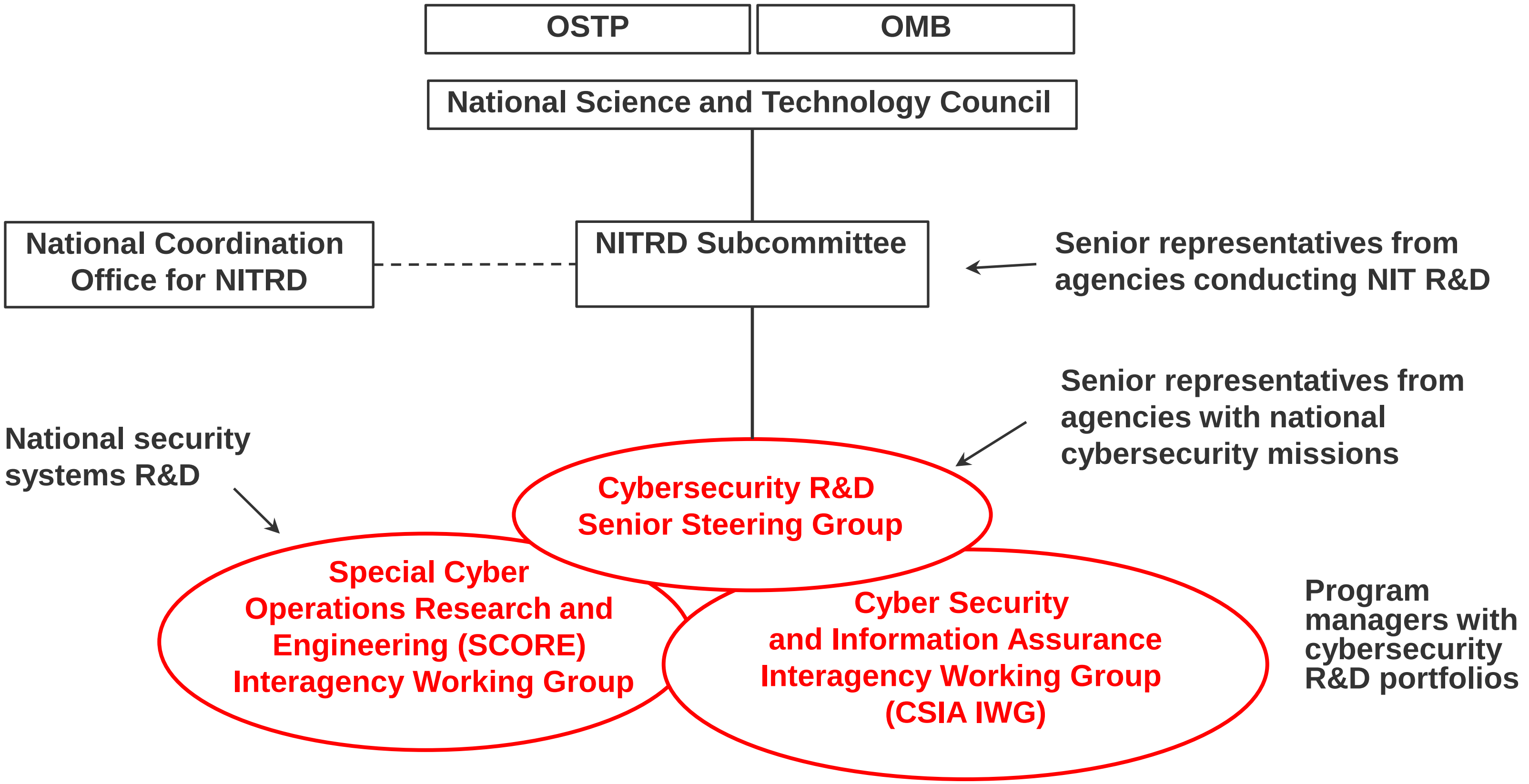
Homeland Security
Science and Technology

http://cybersecurity.whitehouse.gov

NITRD Program

- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Support NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
- Scope
  - Approximately $4B/year across 14 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

NITRD Structure for Cybersecurity R&D Coordination



OSTP

OMB

National Science and Technology Council

National Coordination Office for NITRD

NITRD Subcommittee

Senior representatives from agencies conducting NIT R&D

Senior representatives from agencies with national cybersecurity missions

National security systems R&D

Cybersecurity R&D Senior Steering Group

Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group

Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)

Program managers with cybersecurity R&D portfolios

Federal Cybersecurity Research and Development Program: Strategic Plan

NITRD

NNSA
National Nuclear Security Administration

U.S. Department of Homeland Security

National Science Foundation

National Institutes of Health

NIST
National Institute of Standards and Technology

DARPA

United States Environmental Protection Agency

National Oceanic and Atmospheric Administration
U.S. Department of Commerce

Department of Defense
United States of America

National Security Agency
United States of America

NASA

The National Archives
archives.gov
Democracy Starts Here.

Homeland Security
Science and Technology

Office of Science
U.S. Department of Energy

AHRQ

Federal Gov’t Cyber Research Community

Agency / Org	Research Agenda	Researchers	Customers / Consumers
National Science Foundation (NSF)	Broad range of cyber security topics; Several academic centers	Academics and Non-Profits	Basic Research - No specific customers
Defense Advanced Research Projects Agency (DARPA)	Mostly classified; unclassified topics are focused on MANET solutions	Few academics; large system integrators; research and government labs	Mostly DOD; most solutions are GOTS, not COTS
National Security Agency (NSA)	SELinux; Networking theory; CAEIAE centers	Mostly in-house	Intelligence community; some NSA internal; some open source
Intelligence Advanced Research Projects Agency (IARPA)	Accountable Information Flow (AIF); Large Scale System Defense (LSSD); Privacy Protection Technologies (PPT)	Mostly research labs, system integrators, and national labs; Some academics	Intelligence community
Department of Homeland Security (DHS) S&T	All unclassified; Secure Internet Protocols; Process Control Systems (PCS), Emerging Threats, Insider Threat, Cyber Forensics; Open Security Technologies, Next Generation Technologies, SwA	Blend of academics, research and government labs, non-profits, private sector and small business	DHS Components (including NPPD, NCSC, USCG, FLETC and USSS); CI/KR Sectors; USG and Internet

Homeland Security

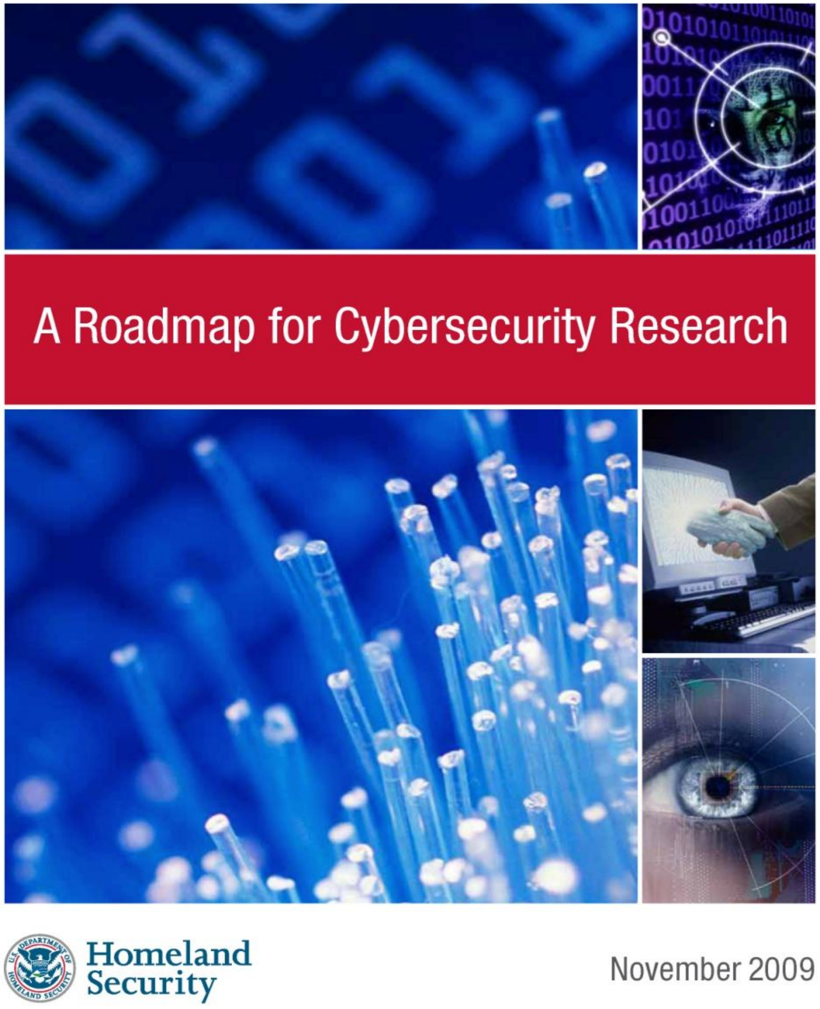
Science and Technology

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

A Roadmap for Cybersecurity Research

- **http://www.cyber.st.dhs.gov**
  - Scalable Trustrworthy 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



A Roadmap for Cybersecurity Research

Homeland Security

November 2009

HSARPA Cyber Security R&D Broad Agency Announcement (BAA) 11-02

- 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

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*

TTA #1: Software Assurance

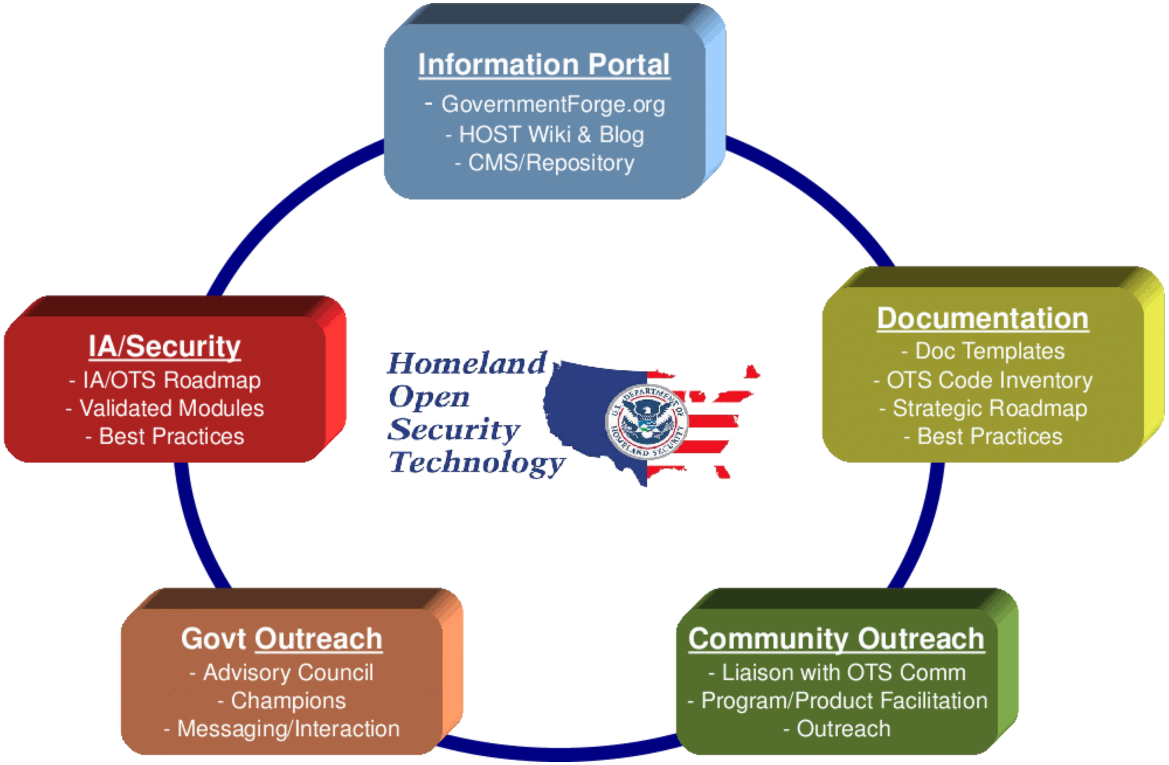
- New tools.
  - Techniques for source code,
  - binary-only techniques,
  - static analysis
  - runtime monitoring techniques
  - Innovative combinations of these techniques were strongly encouraged to synergize the benefits of each while minimizing the difficulties
- Application of new and existing capabilities in test and evaluation activities
  - Large code bases
  - Benchmarking new tools against analysis results previously documented
  - Comprehensive test and evaluation service that applies a broad array of new and existing analysis tools in combination to test and evaluate software across relevant platforms and environments.
- Homeland Open Security Technology (HOST)
  - Government-wide secure information technology (IT) solutions based on open source technologies.
  - Access to vetted open source and related technologies
  - Process of rigorous test and evaluation of software in source and binary form relying heavily on automated processes
- Software Assurance Market Place (TTA #14)

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)

Homeland Open Security Technology (HOST)

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



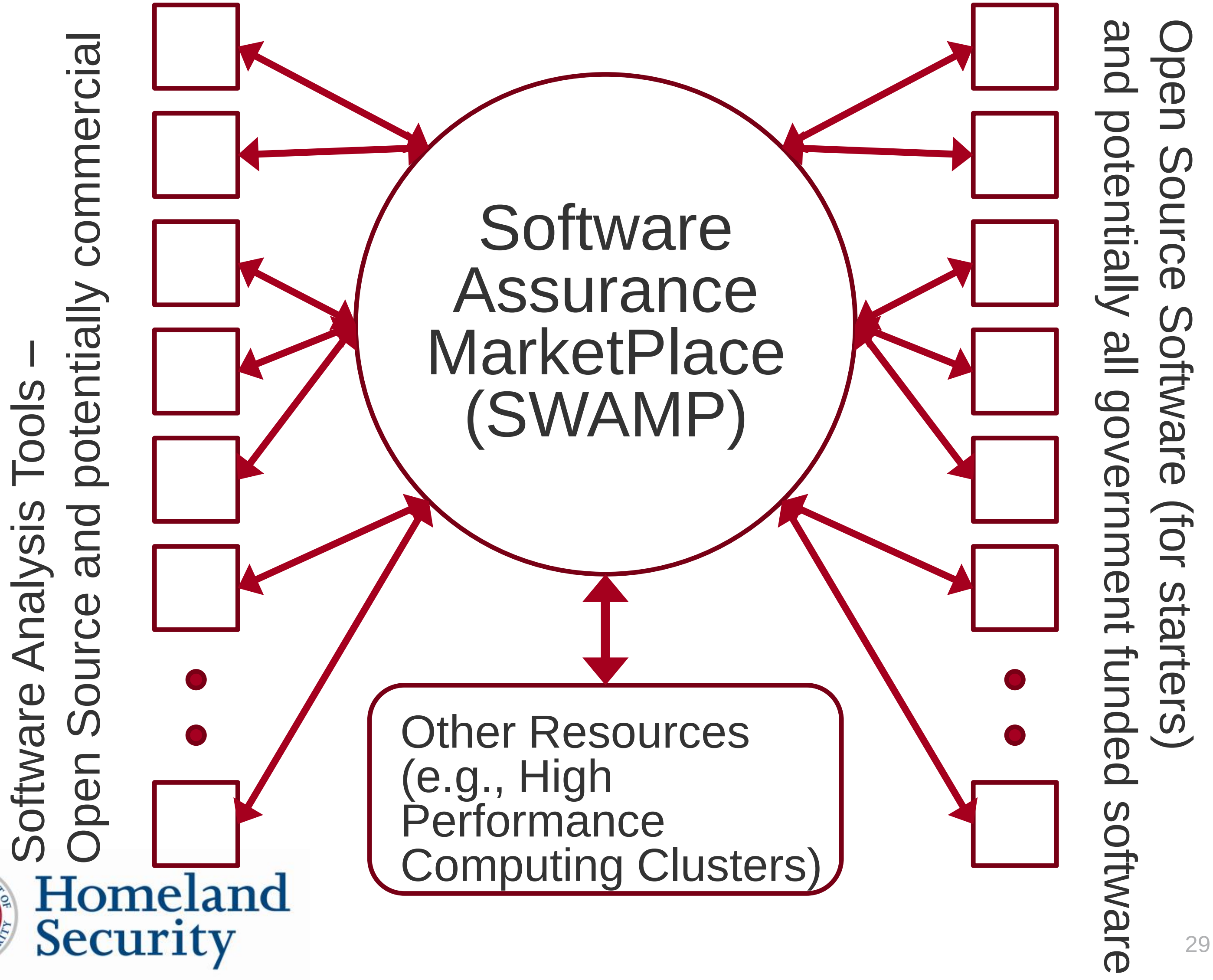
Homeland Security

Science and Technology

Software Assurance - SWAMP

- Focuses on the research infrastructure necessary to enable software quality assurance and related activities.
- A software assurance facility and the associated research infrastructure services that will be made available to both software analysis researchers and software developers, both open source and proprietary.
- DHS expects the SWAMP to become a national level R&D resource in software assurance for open security technologies, used across civilian agencies and their communities as both a research platform and core component supporting US Government supported software development activities.

SWAMP Conceptual Architecture



Software Analysis Tools –
Open Source and potentially commercial

Software Assurance MarketPlace (SWAMP)

Other Resources (e.g., High Performance Computing Clusters)

Open Source Software (for starters)
and potentially all government funded software

Homeland Security

Science and Technology

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

Edward Rhyne

Program Manager

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

edward.rhyne@dhs.gov

202-254-6121

For more information, visit

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

Homeland Security

Science and Technology