DHS S&T CSD Overview – HOST, BAA, SWAMP

Software Assurance Forum
McLean, VA
December 16, 2010

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

2004-2010 S&T Mission

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

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

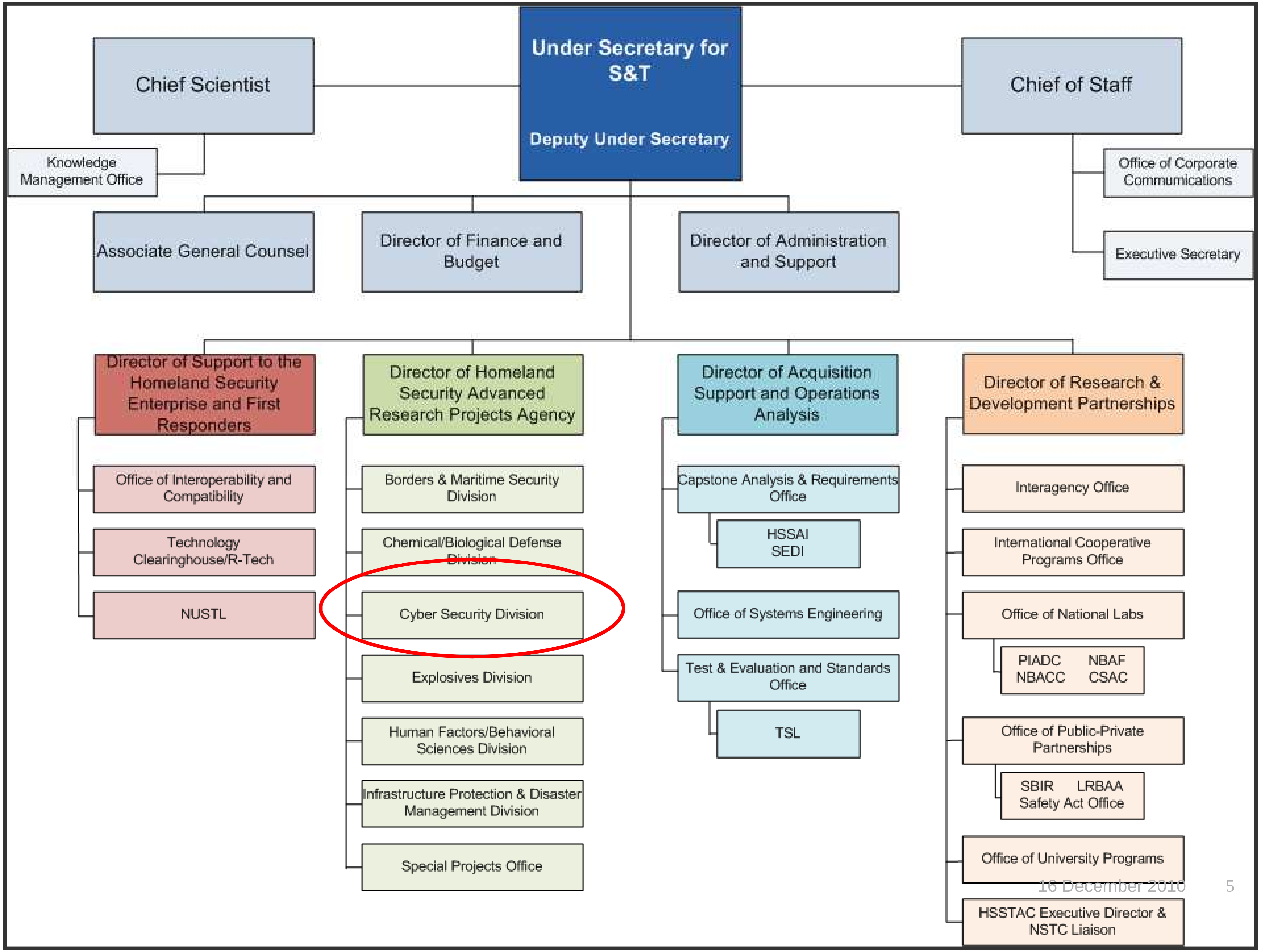
Goal 1: Rapidly develop and deliver knowledge, analyses, and innovative solutions that advance the mission of the Department

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

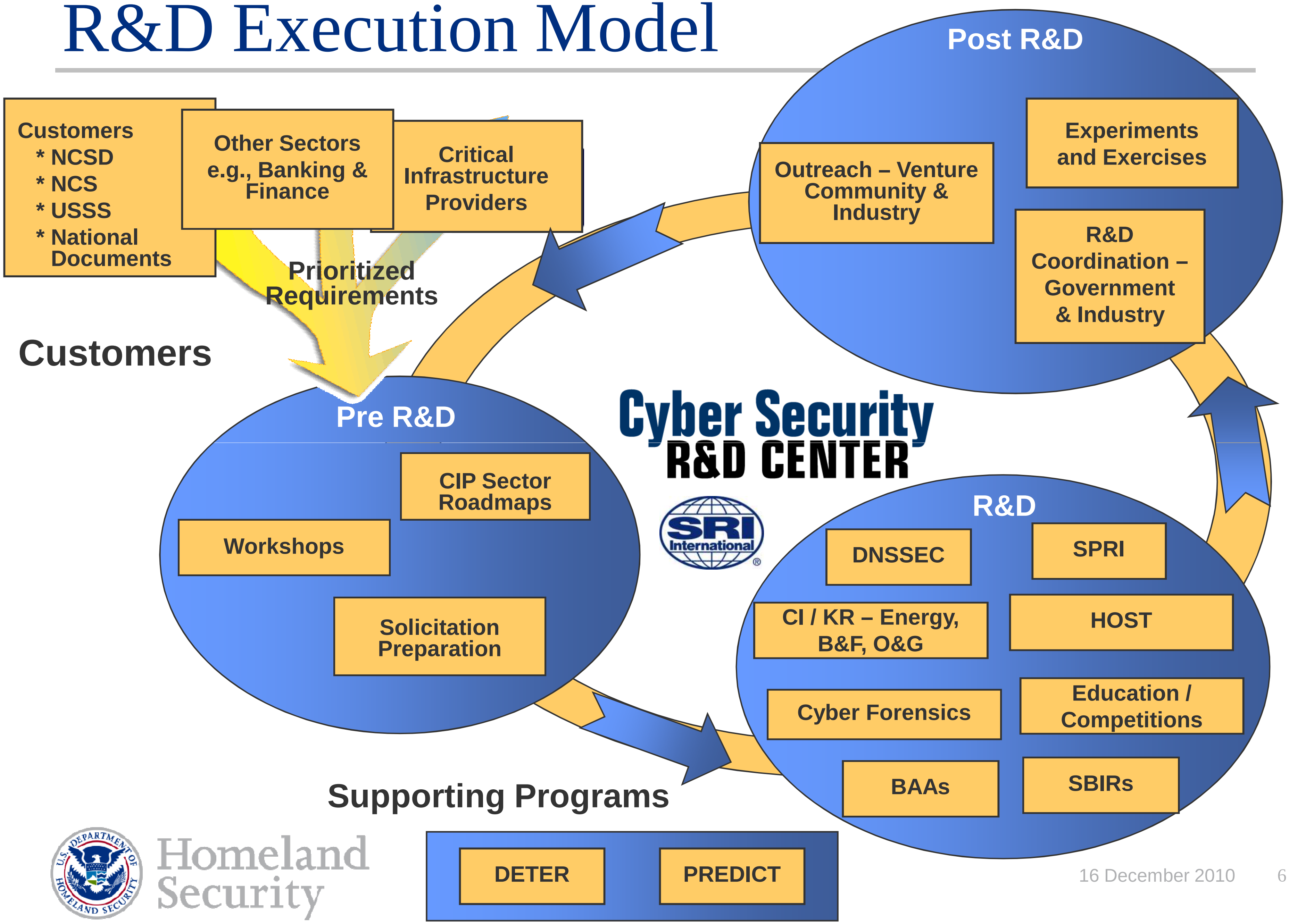


Under Secretary for S&T

Deputy Under Secretary

- Chief Scientist
  - Knowledge Management Office
- Chief of Staff
  - Office of Corporate Communications
  - Executive Secretary
- Associate General Counsel
- Director of Finance and Budget
- Director of Administration and Support
- Director of Support to the Homeland Security Enterprise and First Responders
  - Office of Interoperability and Compatibility
  - Technology Clearinghouse/R-Tech
  - NUSTL
- Director of Homeland Security Advanced Research Projects Agency
  - Borders & Maritime Security Division
  - Chemical/Biological Defense Division
  - Cyber Security Division
  - Explosives Division
  - Human Factors/Behavioral Sciences Division
  - Infrastructure Protection & Disaster Management Division
  - Special Projects Office
- Director of Acquisition Support and Operations Analysis
  - Capstone Analysis & Requirements Office
    - HSSAI
SEDI
  - Office of Systems Engineering
  - Test & Evaluation and Standards Office
    - TSL
- Director of Research & Development Partnerships
  - Interagency Office
  - International Cooperative Programs Office
  - Office of National Labs
    - PIADC NBAF NBACC CSAC
  - Office of Public-Private Partnerships
    - SBIR LRBAA Safety Act Office
  - Office of University Programs
  - HSSTAC Executive Director & NSTC Liaison

R&D Execution Model

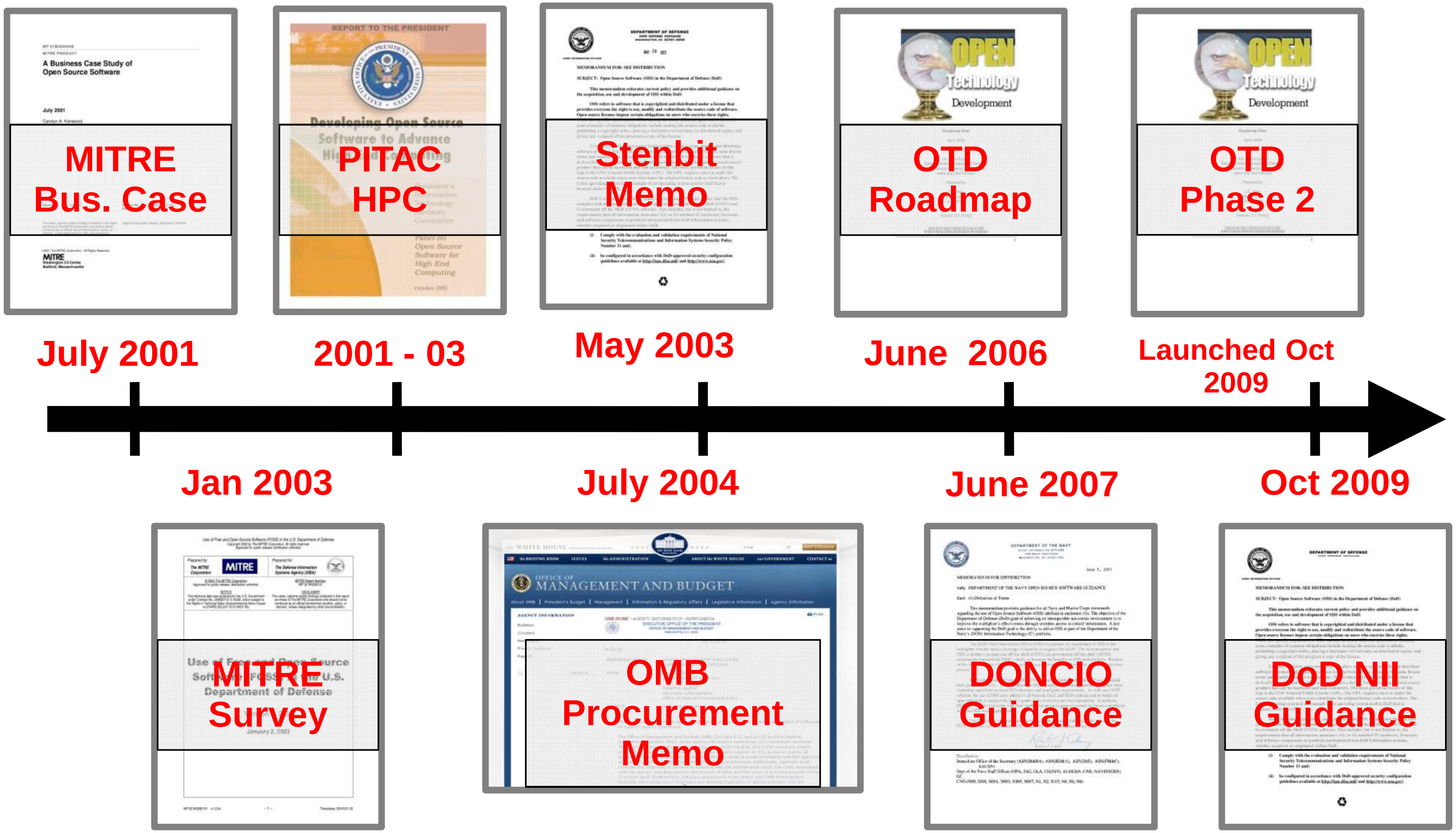


Homeland Security

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
- Exp Deployments, Outreach, Education/Competitions
- Next Generation Technologies
- Small Business Innovative Research (SBIR)
- Research Horizon – What does it look like?

Open Source and Government



July 2001

MITRE Bus. Case

2001 - 03

PITAC HPC

Jan 2003

MITRE Survey

May 2003

Stenbit Memo

July 2004

OMB Procurement Memo

June 2006

OTD Roadmap

June 2007

DONCIO Guidance

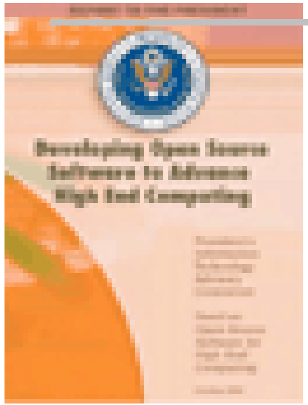
Launched Oct 2009

OTD Phase 2

Oct 2009

DoD NII Guidance

DARPA Program (2001-2003)



Developing Open Source Software to Advance High End Computing

- President’s Information Technology Advisory Committee (PITAC) Report on Open Source Software (OSS) Panel for High Performance Computing (HPC)

Critical Findings

1. Federal government should **encourage the development of Open Source Software**.
2. Federal government should **allow Open Source development efforts to compete on a “level playing field”** with proprietary solutions in government procurement
3. Government sponsored Open Source projects should **choose from a small set of established Open Source licenses** after analysis of each license and determination of which may be preferable.

OpenBSD

Univ. of Pennsylvania

Linux™

WireX Communications

http://www.freebsd.org

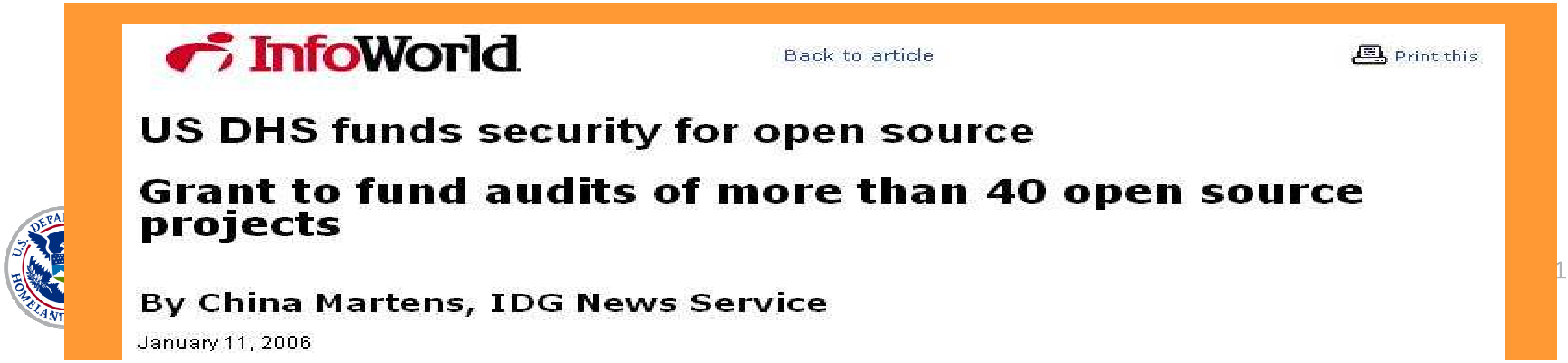
FreeBSD

FreeBSD:The Power To Serve

Network Associates Labs

Coverity: scan.coverity.com

- 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)



US DHS funds security for open source

Grant to fund audits of more than 40 open source projects

By China Martens, IDG News Service

January 11, 2006

Vulnerability Assessment of Open Source “Wireshark”

- **Assessment:** Assess a key open-source monitoring and forensics tool using the University of Wisconsin’s First Principles Vulnerability Assessment (FPVA) methodology
- **Training:** Develop materials and teach tutorials in vulnerability assessment and secure programming techniques
- **Vulnerability characterization and automated detection:** Use the results from assessments to formalize the description of vulnerabilities found and develop algorithms to detect them

Need: Sustainable Government IT Systems

- US Govt Spends $38 Billion on IT Annually
  - Trend is Not Sustainable

- Bureaucracy (easy to blame)
- Complexity of Govt Enterprise Systems
  - Redundancy – Re-Invent the Wheel
- Existing System of Acquisition, Management, Updating, Technical Obsolescence
  - Significant Hurdle

- **Cybersecurity = Protection of Infrastructure and Data**

Approach: Leverage Open Systems

GOAL: Improve systems security, enhance technical efficiency and reduce the cost of IT management...within Govt IT systems.

- **Audience**
  - Federal, State, Local **Government End Users - Citizens**
  - Share Benefits with Industry, Development Communities
- **Open Technology Solutions**
  - Vendor/Platform Agnostic
  - Best of Breed Development – Builds Upon Success
  - Focuses on Addressing the Needs of End Users

Benefits: Open Technology Solutions

- **Open Systems promote and encourage**
  - Transparency – Interoperability – Technical Agility
  - Enhanced Manageability through Open Source License
- **Economic Benefits**
  - Lower Adoption Costs – Promotes Vendor Competition
  - Broad Vendor and Developer Support
  - Secure – Stable – Broadly Adopted in Govt and Industry
- **Existing Govt Adoption/Usage**
  - OMB/White House, DoD, Dept of Navy adoption OS Policy
  - Growing Govt Open Technology Adoption

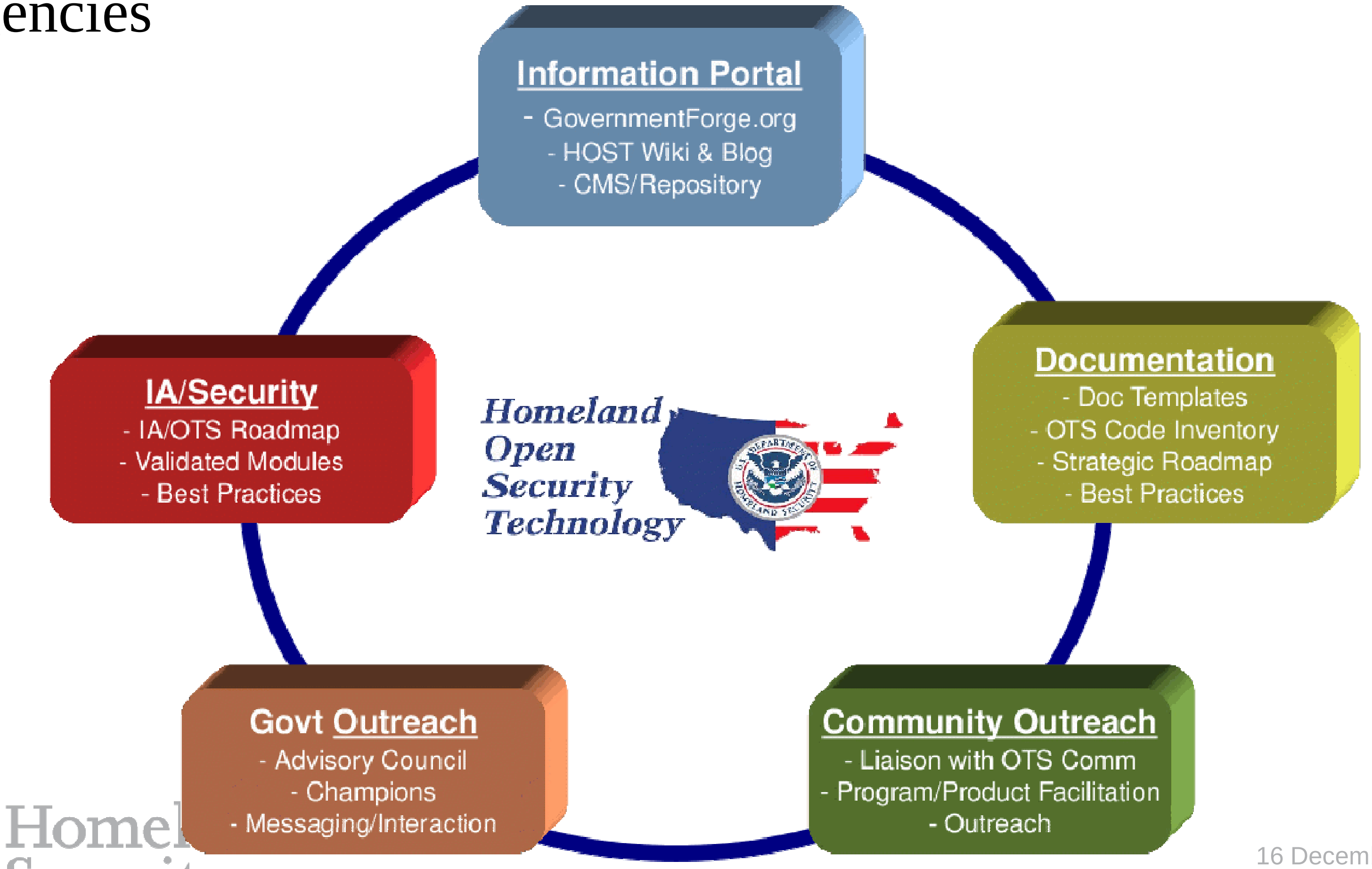
Competition: Who/What are the Challenges

- **Proprietary Vendors**
  - Technology Vendors
  - Business Models
  - Non-competitive solutions

- **Adoption Resistance**
  - Ingrained Systems
  - Existing Relationships
  - Policy Updates and Modifications
  - Change Mentality
  - Lack of Vision, Leadership and Continuity
  - FUD/Pushback

Homeland Open Security Technology (HOST)

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



Information Portal
- GovernmentForge.org
- HOST Wiki & Blog
- CMS/Repository

Documentation
- Doc Templates
- OTS Code Inventory
- Strategic Roadmap
- Best Practices

Community Outreach
- Liaison with OTS Comm
- Program/Product Facilitation
- Outreach

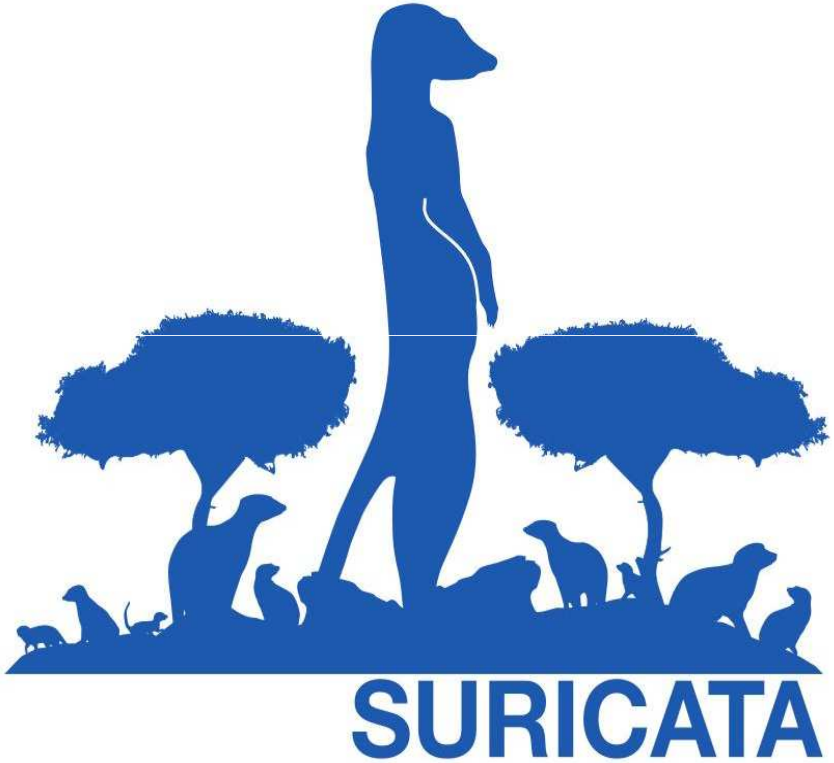
Govt Outreach
- Advisory Council
- Champions
- Messaging/Interaction

IA/Security
- IA/OTS Roadmap
- Validated Modules
- Best Practices

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
  - Looking for other open source “impact” projects
- Information Assurance / Security
  - US Government security evaluation processes (OpenSSL)

HOST - Progress to Date



HOST: Going Forward

- **Investment**
  - $10M up to $50M+
  - 5-yr (1 + 4 w/options)
  - Scalable based on deliverables & program review
- **ROI**
  - Value of Deliverables
  - Strategic Advantage

- **Accountability**
  - Metrics tied to similar IT program of record
    - Investment Costs
    - Recurring Fees
    - Management/Admin Exp
    - Upgrade Costs
    - Compatibility Expenses
    - Vendor Failure Expense
- Process Not Product

Can we afford NOT to Invest in Open Technology?

Next Generation Technologies

- **http://baa.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.

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

- FedBizOpps
  - Look under keyword “cyber”
    - https://www.fbo.gov/index?s=opportunity&mode=form&id=3459d2180c7625e61fff3e2764b7f78d&tab=core&_cview=0
- http://www.cyber.st.dhs.gov
- Industry Day – November 17, 2010 in WDC
- 14 Topics – BAA to be released after Industry Day

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*

Past Solicitations

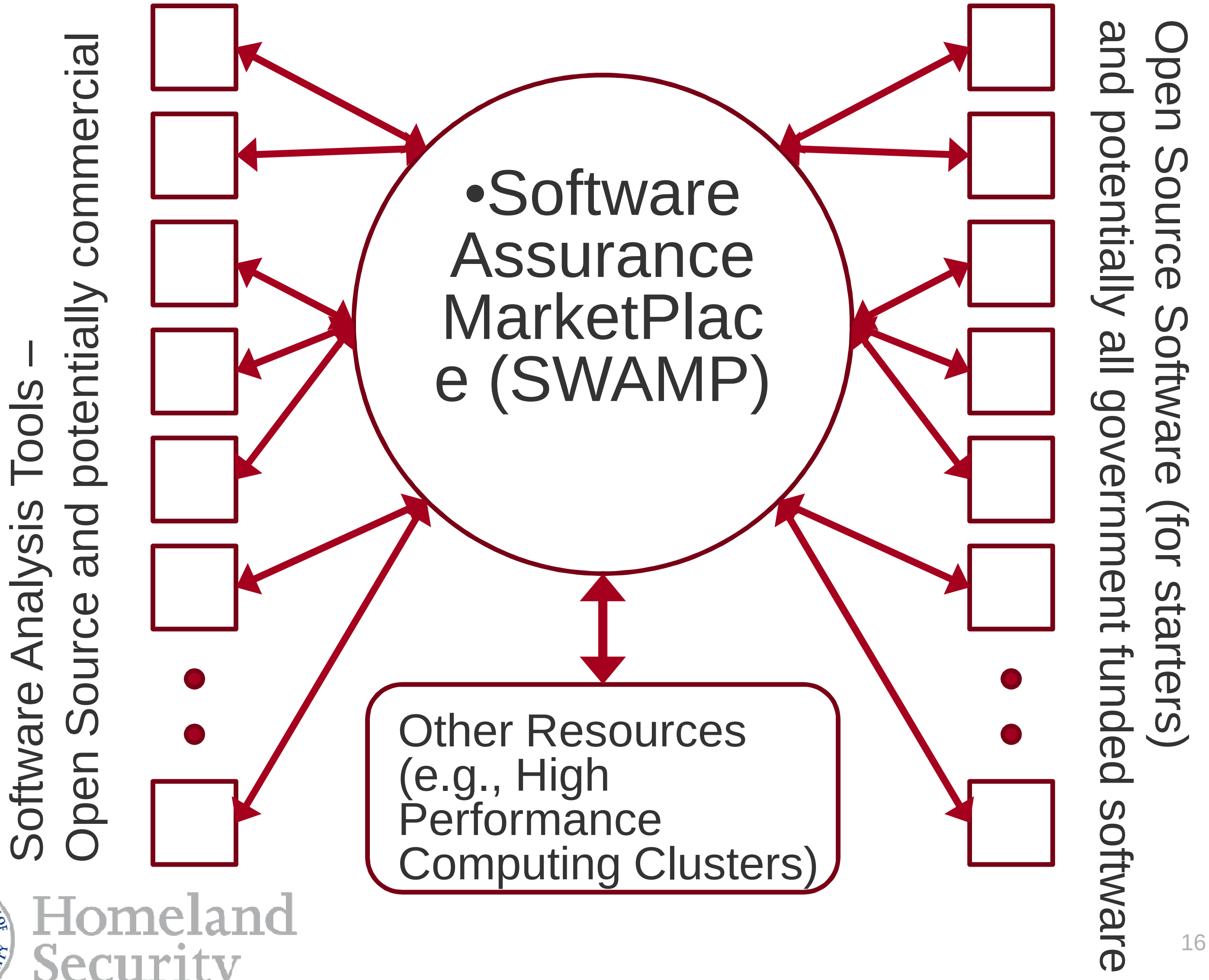
- http://baa.st.dhs.gov
- Left hand side – Past Solicitations
- Look for BAA 07-09 and BAA 04-17

- Review BAA, any modifications or amendments, presentations, etc.
    - Expectation is that BAA 11-XX will be very similar

TTA 14 - Purpose

- Focuses on the research infrastructure necessary to enable software quality assurance and related activities (as solicited in TTA #1)
- 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

TTA 14 – Requirements (1)

- Provide a core cyber infrastructure system Combined hardware and software capable of testing multiple software packages in parallel using multiple software vulnerability analysis tools across multiple and varied platforms. **Multi-platform capability is a requirement.**
- Integrate with available input processes and available normalized output functions
- Web-based accessible service to developers and maintainers of open source and potentially others
- An Initial Operating capability (IOC) for this system is expected within 15 months of the start of activities

TTA 14 – Requirements (2)

- Do not address tool development (TTA #1). Discuss how tools will be incorporated into the research infrastructure
- Address access to computing resources, especially when considering scaling and performance of the system in usage scenarios involving multiple and simultaneous users testing multiple source code packages in a multi-platform environment. Address long term R&D operations issues.
- Leverage standards, reference material, and functional capabilities that already exist or are under active developmentSAFES, CWE, CVE, CAPEC, NIST’s NVD, SCAP, NSRL, TOIF

TTA 14 – Requirements (3)

- Funding profile: up to $5M in Year 1; up to $5M in Year 2; and option years for up to three additional years at undetermined limits. Explain operations and maintenance costs for R&D infrastructure in years 3-5
- Program seeks to couple activities funded in this TTA with HOST
  - Goal is to facilitate Government-wide secure IT solutions based on open source technologies. More information on HOST can be found at http://www.cyber.st.dhs.gov. Responses in this TTA are encouraged to consider how their activities will integrate with the HOST program.

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