Homeland Security Advanced Research Projects Agency

Cyber Security Division

Douglas Maughan, Ph.D.
Director

July 26, 2012

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

- Homeland Security Act 2002
- QHSR (Feb 2010)
- NIPP (2009)
- BUR (July 2010)
- S&T Strategic Plan (2011)

**Operational Directives**

- PPD-8 National Preparedness (2011)

**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

**PPD-8 National Preparedness System: Prevention, Protection, Mitigation, Response, Recovery**
Comprehensive National Cybersecurity Initiative (CNCI)

<table>
<thead>
<tr>
<th>Focus Area 1</th>
<th>Establish a front line of defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the Number of Trusted Internet Connections</td>
<td>Deploy Passive Sensors Across Federal Systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Focus Area 2</th>
<th>Resolve to secure cyberspace / set conditions for long-term success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Current Centers to Enhance Situational Awareness</td>
<td>Develop Gov’t-wide Counterintelligence Plan for Cyber</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Focus Area 3</th>
<th>Shape future environment / secure U.S. advantage / address new threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define and Develop Enduring Leap Ahead Technologies, Strategies &amp; Programs</td>
<td>Define and Develop Enduring Deterrence Strategies &amp; Programs</td>
</tr>
</tbody>
</table>

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
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
CSD R&D Execution Model

Critical infrastructure owners and operators

DHS customers

Prioritized requirements

Post-R&D
- Experiments
- Tech transfer

Pre-R&D
- Workshops
- Solicitations

R&D
- Program support

Cyber Security R&D CENTER
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
  - Several commercial customers; Government pilots underway

- 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
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)
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](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](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
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
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)
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
DHS S&T Cybersecurity Program

PEOPLE

Identity Management
Enterprise Level Security Metrics & Usability
Data Privacy
Cyber Forensics
Competitions

SYSTEMS

Secure Protocols
Process Control Systems
Internet Measurement & Attack Modeling

INFRASTRUCTURE

Cyber Economic Incentives
Moving Target Defense
Tailored Trustworthy Spaces
Leap Ahead Technologies
Transition To Practice

Software Quality Assurance
Homeland Open Security Technology
Experiments & Pilots
Assessments & Evaluations

RESEARCH INFRASTRUCTURE

Experimental Research Testbed (DETER)
Research Data Repository (PREDICT)
Software Assurance Market Place (SWAMP)
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

<table>
<thead>
<tr>
<th>Type I (New Technologies)</th>
<th>Type II (Prototype Technologies)</th>
<th>Type III (Mature Technologies)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Development Phase</td>
<td>✓ Development Phase</td>
<td>✓ Demo Only in Op Environ.</td>
</tr>
<tr>
<td>✓ Funding ≤ $3M &amp; 36 mos.</td>
<td>✓ Funding ≤ $2M &amp; 24 mos.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Technology Demonstrations = Test, Evaluation, and Pilot deployment in DHS “customer” environments
## BAA 11-02 Technical Topic Areas (TTAs)

<table>
<thead>
<tr>
<th>TTA-1</th>
<th>Software Assurance</th>
<th>DHS, FSSCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTA-2</td>
<td>Enterprise-Level Security Metrics</td>
<td>DHS, FSSCC</td>
</tr>
<tr>
<td>TTA-3</td>
<td>Usable Security</td>
<td>DHS, FSSCC</td>
</tr>
<tr>
<td>TTA-4</td>
<td>Insider Threat</td>
<td>DHS, FSSCC</td>
</tr>
<tr>
<td>TTA-5</td>
<td>Resilient Systems and Networks</td>
<td>DHS, FSSCC</td>
</tr>
<tr>
<td>TTA-6</td>
<td>Modeling of Internet Attacks</td>
<td>DHS</td>
</tr>
<tr>
<td>TTA-7</td>
<td>Network Mapping and Measurement</td>
<td>DHS</td>
</tr>
<tr>
<td>TTA-8</td>
<td>Incident Response Communities</td>
<td>DHS</td>
</tr>
<tr>
<td>TTA-9</td>
<td>Cyber Economics</td>
<td>CNCI</td>
</tr>
<tr>
<td>TTA-10</td>
<td>Digital Provenance</td>
<td>CNCI</td>
</tr>
<tr>
<td>TTA-11</td>
<td>Hardware-Enabled Trust</td>
<td>CNCI</td>
</tr>
<tr>
<td>TTA-12</td>
<td>Moving Target Defense</td>
<td>CNCI</td>
</tr>
<tr>
<td>TTA-13</td>
<td>Nature-Inspired Cyber Health</td>
<td>CNCI</td>
</tr>
<tr>
<td>TTA-14</td>
<td>Software Assurance MarketPlace (SWAMP)</td>
<td>S&amp;T</td>
</tr>
</tbody>
</table>

- 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
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)
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

<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>NRC CSTB Trust in Cyberspace</td>
</tr>
<tr>
<td>1999</td>
<td>National Strategy to Secure Cyberspace</td>
</tr>
<tr>
<td>2000</td>
<td>NIAC Hardening the Internet</td>
</tr>
<tr>
<td>2001</td>
<td>PITAC – Cyber Security: A Crisis of Prioritization</td>
</tr>
<tr>
<td>2002</td>
<td>IRC Hard Problems List</td>
</tr>
<tr>
<td>2003</td>
<td>NSTC Federal Plan for CSIA R&amp;D</td>
</tr>
<tr>
<td>2004</td>
<td>NRC CSTB Toward a Safer and More Secure Cyberspace</td>
</tr>
<tr>
<td>2005</td>
<td>NSPD-54/HSPD-23</td>
</tr>
<tr>
<td>2006</td>
<td>White House Cyberspace Policy Review</td>
</tr>
<tr>
<td>2007</td>
<td>DHS S&amp;T Roadmap for Cybersecurity Research</td>
</tr>
<tr>
<td>2008</td>
<td>Trustworthy Cyberspace – Federal Cybersecurity R&amp;D Strategic Plan</td>
</tr>
</tbody>
</table>

All documents available at: [http://www.cyber.st.dhs.gov/resources/](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
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