Homeland Security Advanced Research Projects Agency

Government Support for Transition – Where can you find it?

Douglas Maughan, Ph.D.
Division Director

November 28, 2012

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

Homeland Security
Science and Technology

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

FOCUS AREAS

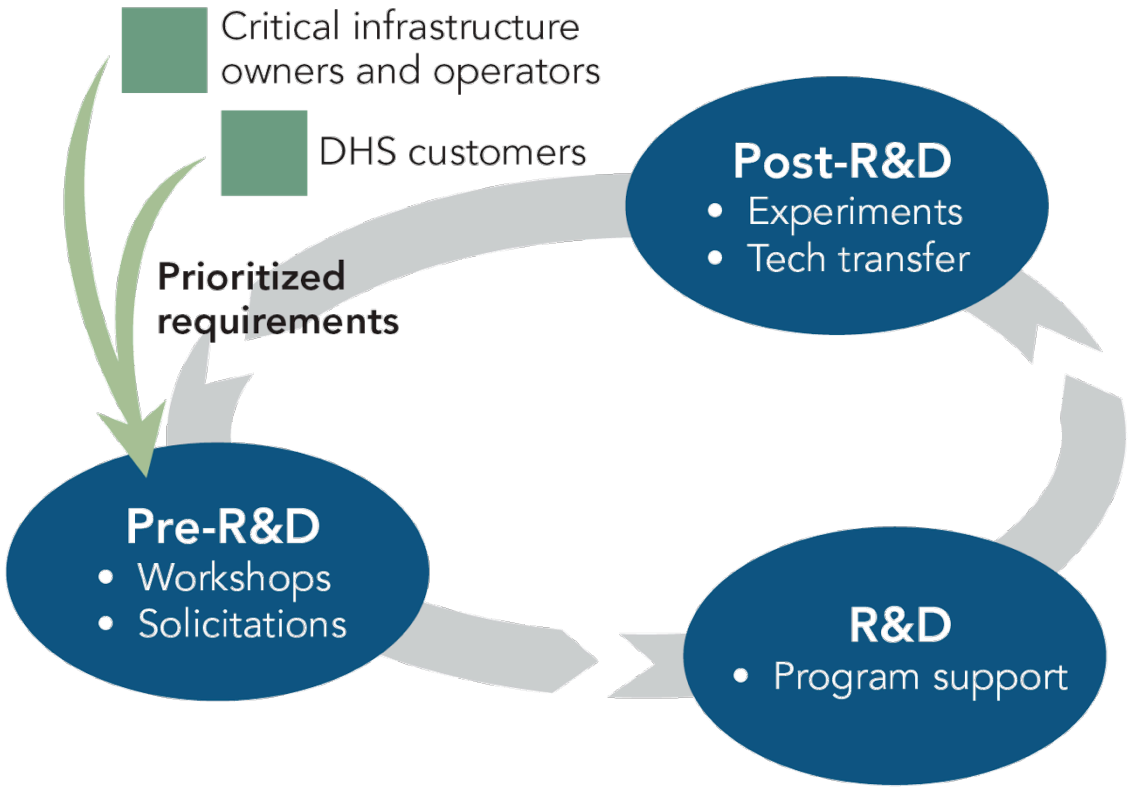
- Bio
- Explosives
- Cybersecurity
- First Responders

Homeland Security

Science and Technology

Homeland Security
Science and Technology

CSD R&D Execution Model



Research
Development
Test and Evaluation &
Transition (RDTE&T)

Successes

- Ironkey – Secure USB
  - Standard Issue to S&T employees from S&T CIO
  - Acquired by Imation
- 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

Homeland Security
Science and Technology

Programs for U. S. Small Business

- **Small Business Innovation Research (SBIR)** **2.5%**

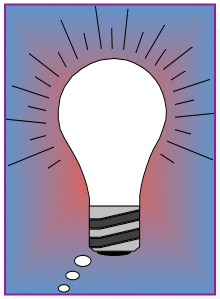
  Set-aside program for small business concerns to engage in federal R&D -- with potential for commercialization

- **Small Business Technology Transfer (STTR)** **.3%**

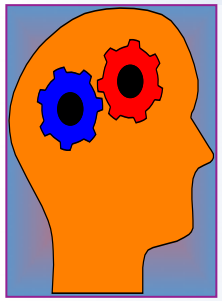
  Set-aside program to facilitate cooperative R&D between small business concerns and research institutions -- with potential for commercialization

Homeland Security
Science and Technology

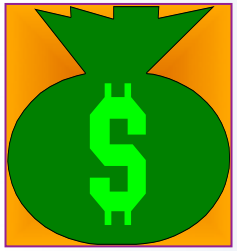
SBIR - A 3 Phase Program



- **PHASE I**
  - Feasibility Study
  - $100K (in general) and 6 month effort (amounts are changing)



- **PHASE II**
  - Full Research/R&D
  - $750K and 24 month effort (amounts are changing)
  - Commercialization plan required



- **PHASE III**
  - Commercialization Stage
  - Use of non-SBIR Funds

Homeland Security
Science and Technology

Agency SBIR Differences

- ❑Number and timing of solicitations
- ❑R&D Topic Areas – Broad vs. Focused
- ❑Dollar Amount of Award (Phase I and II)
- ❑Proposal preparation instructions
- ❑Financial details (e.g., Indirect Cost Rates)
- ❑Proposal review process
- ❑Proposal success rates
- ❑Types of award
- ❑Commercialization assistance
- ❑And more……

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

HOST Program

Homeland Security
Science and Technology

HOST = Homeland Open Security Technology

Closing government cybersecurity gaps by sponsoring open source projects

- Suricata Intrusions Detection System
- OpenSSL FIPS validation

...and helping government be able to find and deploy existing open source cybersecurity solutions

- Inventory of solutions, **opencybersecurity.org**
- Use cases & lessons learned reports
- Improved policy

Open Information Security Foundation and Suricata

Homeland Security
Science and Technology

- A new model for managing and sustaining innovation
  - A non-profit to develop and “own” the code
  - Software Freedom Law Center created the License pro bono
  - A consortium of companies providing support in exchange for not having to release changes
- Ground-up rewrite
  - Multi-Threaded
  - Automated Protocol Detection
  - File Identification and Extraction
  - GPU Acceleration

bivio networks
npulse TECHNOLOGIES
QUALYS
intel
nitrosecurity
KERIO
BREACH SECURITY LABS
endace
EVERIS The Cornerstone of Network Security
NVIDIA TESLA WITH CUDA
napatech

~$1.2m in DHS funding was matched by ~$8m in commercial sponsorship

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

TTP Program Focus Areas

Identify

- Identify cyber security research that is at Technical Readiness Level (TRL) 5 or higher that can be projected into the Homeland Security Enterprise and beyond

Implement

- Partner with the IT operations groups within the Homeland Security Enterprise to pilot the cybersecurity technologies that are identified

Introduce

- Partner with the private sector to commercialize technology to bring the innovation to a broader audience

Transition To Practice Program Focus

R&D Sources

- DOE National Labs
- FFRDC's (Federally Funded R&D Centers)
- Academia
- Small Business

Transition processes

- Testing & evaluation
- Red Teaming
- Pilot deployments

Utilization

- Open Sourcing
- Licensing
- New Companies
- Adoption by cyber operations analysts
- Direct private-sector adoption
- Government use

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
  - **There will be a new solicitation for 2013**
- 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.

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