DHS S&T Cybersecurity R&D Activities: A Review, Update and Discussion

Douglas Maughan, Ph.D.

Division Director

April 8, 2014

Homeland Security
Science and Technology

Presentation Outline

- Review Interactions Between Cyber Security Division (CSD) and HSSTAC
  - July 2008
  - December 2008 HSSTAC Assessment Report
  - Sept 2010
  - CSD officially created in Nov 2010
  - Jan 2011
  - Jan 2013
  - **Describing:**
    - Political / Strategic Landscape
    - Technical Program
    - Resources – People and Budget
- CSD Today and in the Future
- Summary and Observations

Homeland Security
Science and Technology

2007 Hearings in Washington

(Discussed with HSSTAC July 2008)

- **Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure**
  - http://homeland.house.gov/hearings/index.asp?ID=36
- **Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action"**
  - http://homeland.house.gov/hearings/index.asp?ID=41
- **House Homeland Security Committee investigation of DHS Networks**
  - http://homeland.house.gov/SiteDocuments/Charbo.pdf
- **Senate Hearing on Terrorist use of the Internet**
  - http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=441

Homeland Security
Science and Technology

Other recent "Attention"

(Discussed with HSSTAC July 2008)

- May 2007 – DDOS attack on Estonia
  - First example of "cyber warfare"?
- Sep 2007 - "Chinese hack the Pentagon"
- Sep 2007 – "China hacks UK government"
- Oct 2007 – "White House initiative to defend against hackers"
- Nov 2007 – "White House requests $154M supplement for Cyber Initiative"

Homeland Security
Science and Technology

Cyber Security Program Areas

(Discussed with HSSTAC July 2008)

- Information Infrastructure Security
  - Domain Name System Security (DNSSEC)
  - Secure Protocols for the Routing Infrastructure (SPRI)
  - Cyber Security Assessment
- Cyber Security Research Tools and Techniques
  - Cyber Security Testbed (DETER)
  - Large Scale Datasets (PREDICT)
  - Experiments and Exercises
- Next Generation Technologies
  - BAA 04-17: 17 Awards – 5 still active, 12 completed
  - BAA 07-09: 14 Awards – 14 awarded
- Other Activities (SBIR, RTAP, Emerging Threats, Outreach, Government Coordination)

Homeland Security
Science and Technology

Cyber Security Budget Overview

(Discussed with HSSTAC July 2008)

- FY03 …… $3M
- FY04 …… $10M
- FY05 …… $18M
- FY06 …… $16.5M
- FY07 …… $13M
- FY08 …… $18.7M

2 Federal Employees

- 3 Contractors

Homeland Security
Science and Technology

HSSTAC Dec. 2008 Report

- Reviewed most Government R&D organizations
- 9 Findings
  - Threat continues to grow; Progress will take time
  - National policies still being developed; CONOPS immature
  - Need connections between S&T and operational organizations
  - Shortfall of qualified personnel to address cybersecurity challenges
- 9 Recommendations
  - USST work with operational organization to agree relationships
  - S&T continue current investment and expand it
  - Begin program of technology validation and verification
  - Create program to increase number of engineers and scientists
  - Begin program for analysts to manage volumes of data
  - Begin program in rapid forensics and attribution

Homeland Security
Science and Technology

Comprehensive National Cyber Initiative (CNCI) Programs

(Discussed with HSSTAC Sept 2010)

- Focus Area 1 - Establish a front line of defense
  - Reduce the Number of Trusted Internet Connections (*FNS-DNSSEC)
  - Deploy Passive Sensors Across Federal Systems (*US-CERT)
  - Pursue Deployment of Automated Defense Systems (*RFI Review)
  - Coordinate and Redirect R&D Efforts (**SSG Member)
- Focus Area 2 - Resolve to secure cyberspace / set conditions for long-term success
  - Connect Current Centers to Enhance Situational Awareness (NCSC Support)
  - Develop Gov't-wide Counterintelligence Plan for Cyber
  - Increase Security of the Classified Networks
  - Expand Education (*NCSD Ed/Train)
- Focus Area 3 - Shape future environment /secure U.S. advantage/address new threats
  - Define and Develop Enduring Leap Ahead Technologies, Strategies & Programs (**CSIA IWG Co-Chair)
  - Define and Develop Enduring Deterrence Strategies & Programs
  - Manage Global Supply Chain Risk
  - Cyber Security in Critical Infrastructure Domains (*CSCSWG)

** S&T Indirect Involvement*

*** S&T Direct Involvement*

Cyber Security Program Areas 2010

(Discussed with HSSTAC Sept 2010)

- Information Infrastructure Security
- Cyber Security Research Infrastructure
- Next Generation Technologies
  - Two new program areas – Cyber Forensics and Homeland Open Security Technology (HOST)
- Small Business Innovative Research (SBIR)
- Experimental Deployments
- Outreach and Education/Competitions
- Research Horizon – What does it look like?

Homeland Security
Science and Technology

A Roadmap for Cybersecurity Research

(Discussed with HSSTAC Sept 2010)

Report posted at: 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
Science and Technology

Cyber Security Budget Overview 2010

(Discussed with HSSTAC Sept 2010)

- FY03 …… $3M
- FY04 …… $10M
- FY05 …… $18M
- FY06 …… $16.5M
- FY07 …… $13M
- FY08 …… $18.7M
- FY09 …… $29.3M
- FY10 …… $41.7M

Homeland Security
Science and Technology

Cyber Security Program Areas (2011)

(Discussed with HSSTAC Jan 2011)

- 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)

Homeland Security
Science and Technology

Cyber Security Budget Overview (2011

(Discussed with HSSTAC Jan. 2011)

- FY03 …… $3M
- FY04 …… $10M
- FY05 …… $18M
- FY06 …… $16.5M
- FY07 …… $13M
- FY08 …… $18.7M
- FY09 …… $29.3M
- FY10 …… $41.7M
- FY11 …… $44.0M

Homeland Security
Science and Technology

Fed Cybersecurity R&D Strategic Plan

(Discussed with HSSTAC Jan. 2013)

Plan Released December 6, 2011

- Science of Cyber Security
- Research Themes
  - Tailored Trustworthy Spaces
  - Moving Target Defense
  - Cyber Economics and Incentives
  - Designed-In Security (New for FY13)
- 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

Cyber Security R&D Broad Agency Announcement (BAA)

(Discussed with HSSTAC Jan. 2013)

- 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 1 (New Technologies) – Applied Research Phase, Development Phase, Demo in Op Environ. Funding < $3M & 36 months
  - Type II (Prototype Technologies) – More Mature Prototypes, Development Phase, Demo in Op Environ., Funding <$2M & 24 months
  - Type III (Mature Technologies) – Mature Technology, Demo Only in Op. Environ. Funding <$750K &12 months

Note: Technology Demonstrations = Test, Evaluation, and Pilot development in DHS "customer" environments

Homeland Security
Science and Technology

BAA 11-02 Technical Topic Areas (TTAs)

(Discussed with HSSTAC Jan. 2013)

- 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

1003 White Papers – 224 Full Proposals encouraged – 36 Awards (Sept/Oct 2012)

S&T International Engagements

(Discussed with HSSTAC Jan 2013)

- International Bilateral Agreements
  - Government-to-government cooperative activities for 13 bilateral Agreements
  - Over $6M of International co-funding
    - Canada (2004) - 11 projects, $1.8M money in, $0 joint, $0 money out
    - Australia (2004) – 3 projects, $300K money in, $400K Joint, $0 money out
    - United Kingdom (2005) – 3 projects, $1.2M money in, $400K joint, $0 money out
    - Singapore (2007)
    - Sweden (2007) - 4 projects, $650K money in, $0 joint, $0 money out
    - Mexico (2008)
    - Israel (2008) – 2 projects, $0 money in, $100K joint, $0 money out
    - France (2008)
    - Germany (2009) – 1 project, $0 money in, $300K joint, $0 money out
    - New Zealand (2010)
    - European Commission (2010) – 1 project
    - Spain (2011)
    - Netherlands (2013) – 7 projects, $450K money in, $1.2M joint, $150K money out
    - Japan – 1 project

Note: This slide was converted from the original graphic to text only in order to meet 508 compliance. For the original graphic, contact Mary Hanson, mary.hanson@hq.dhs.gov.

Homeland Security
Science and Technology

Cyber Security Budget Overview (2013)

(Discussed with HSSTAC Jan 2013)

- FY03 …… $3M
- FY04 …… $10M
- FY05 …… $18M
- FY06 …… $16.5M
- FY07 …… $13M
- FY08 …… $18.7M
- FY09 …… $29.3M
- FY10 …… $41.7M
- FY11 …… $44.0M
- FY12 …… $44.7M
- FY13 …… $69.8M

Homeland Security
Science and Technology

CSD Issues Discussion

(Discussed with HSSTAC Jan 2013)

- Provided 20 questions to HSSTAC in the following areas:
  - Technical Focus areas for the next 3-5 years
  - Public-Private Partnerships
  - Continued Focus on the full R&D lifecycle
  - Workforce and Educational Activities
  - DHS Component Engagement
  - Organizational Size, Structure, and Positioning
  - Miscellaneous – Metrics, Accountability, Outreach
- Not enough interaction or discussion between HSSTAC and CSD on these issues

Homeland Security
Science and Technology

CSD Today and in the Future

- Organization:
  - 12 Federal Employees
  - 2 IPAs
  - 14 contractors

Homeland Security
Science and Technology

Cyber Security Budget Overview

- FY03 …… $3M
- FY04 …… $10M
- FY05 …… $18M
- FY06 …… $16.5M
- FY07 …… $13M
- FY08 …… $18.7M
- FY09 …… $29.3M
- FY10 …… $41.7M
- FY11 …… $44.0M
- FY12 …… $44.7M
- FY13 …… $69.8M
- FY14 …… $70.2M (Enacted)

Homeland Security
Science and Technology

Cyber Threats and Sources

- Malware – Malicious software to disrupt computers
- Viruses, worms, …
- Theft of Intellectual Property or Data
- Hactivism – Cyber protests that are socially or politically motivated
- Mobile Devices and Applications and their associated Cyber Attacks
- Social Engineering – Entice users to click on Malicious Links
- Spear Phishing – Deceptive communications (E-Mails, Texts, Tweets)
- Domain Name System (DNS) Hijacking
- Router Security – Border Gateway Protocol (BGP) Hijacking
- Denial of Service (DOS) – blocking access to web sites
- Others …..

Homeland Security
Science and Technology

White House Priorities – FY14+

- Secure Federal Networks
  - Identity/Credential Access Mgmt (ICAM), Cloud Exchange, Fed-RAMP
- Protect Critical Infrastructure
  - Public-Private Cyber Coordination, EO/PPD Initiatives
- Improve Incident Response and Reporting
  - Information Sharing among Federal Centers
  - Capacity Building for State/Local/Tribal/Territorial (SLTTs)
- Engage Internationally
  - Foreign Assistance Capacity Building
  - Build Workforce Capacity to Support International Cyber Engagement
- Shape the Future
  - National Strategy for Trusted Identity in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)
  - Cybersecurity R&D – EO/PPD R&D Plan, Federal R&D Plan, Transition To Practice, Foundational Research

Homeland Security
Science and Technology

U.S. Federal Cybersecurity Operations Team
National Roles and Responsibilities

- The original slide for this location was a graphic that does not meet 508 compliance. It shows the national roles and responsibilities of the U.S. federal cybersecurity operations team, which is comprised of three federal agencies: DOJ/FBI, DHS, and DoD. DOJ/FBI has the lead for investigation and enforcement, DHS has the lead for protection, and DoD has the lead for national defense. The intelligence community focuses on cyber threat intelligence and attribution, and interacts with all three agencies. For the original graphic, contact Mary Hanson, mary.hanson@hq.dhs.gov

Homeland Security
Science and Technology

Executive Order (EO) on Improving Critical Infrastructure Cybersecurity/ Policy Presidential Directive (PPD) on Critical Infrastructure Security and Resilience

Executive Order 13636: Improving Critical Infrastructure Cybersecurity directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote/incentivize adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore existing regulation to promote cyber security

Presidential Policy Directive-21: Critical Infrastructure

- Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

"America must also face the rapidly growing threat from cyber attacks… That's why, earlier today, I signed a new executive order that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy." - President Barack Obama, 2013 State of the Union

Homeland Security
Science and Technology

Cyber Security Thrust Areas

- CNCI and Federal R&D Plan Programs
  - Executing R&D programs with support from WH, OMB, OSTP
- Trustworthy Cyber Infrastructure
  - Working with the global Internet and critical infrastructure communities to secure cyberspace
- Research Infrastructure to Support Cybersecurity
  - Supporting national-level research with necessary R&D infrastructure
- Network and System Security
  - Technologies for next-generation networks and systems
- Law Enforcement R&D Needs
  - Capabilities to support F/S/L law enforcement requirements
- Cybersecurity Education
  - Leading National and DHS cybersecurity education initiatives, including Cyber Skills Task Force (CSTF)

Homeland Security
Science and Technology

CSD Resource Allocations

HSARPA FY14 Core and Potential HSARPA FY14/15 New Starts (Combined):

- Comprehensive National Cybersecurity Initiative (CNCI)
  - Approximately $18M
- Trustworthy Cyber Infrastructure
  - Approximately $20M
- Research Infrastructure
  - Approximately $7.5M
- Network and System Security
  - Approximately $37M
- Law Enforcement R&D Needs
  - Approximately $11M
- Cyber Education
  - Approximately $8M

NOTE: This slide was converted from the original graphic to text only in order to meet 508 compliance. For the original graphic, contact Mary Hanson, mary.hanson@hq.dhs.gov

Homeland Security
Science and Technology

R&D Partnerships

- Oil and Gas Sector
  - LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity
- Electric Power Sector
  - TCIPG – Trustworthy Computing Infrastructure for the Power Grid
- Banking and Finance Sector
  - FI-VICS – Financial Institutions – Verification of Identity Credential Service
  - DECIDE – Distributed Environment for Critical Incident Decision-making Exercises (recent Quantum Dawn II exercise)
- State and Local
  - PRISEM - Public Regional Information Security Event Management
  - PIV-I/FRAC TTWG – State and Local and Private Sector First Responder Authentication Credentials and Technology Transition
- Law Enforcement
  - SWGDE – Special Working Group on Digital Evidence (FBI lead)
  - CFWG – Cyber Forensics Working Group (CBP, ICE, USSS, FBI, S/L)
- S2ERC - Security and Software Engineering Research Center
  - 15+ gov't and industry partners; 12 academics; collaborative R&D

Homeland Security
Science and Technology

Transition To Practice (TTP) Program

- R&D Sources: DOE National Labs, FFRDC's (Federally Funded R&D Centers), Academia, Small Business
- Transition Process: Testing & evaluation, Red Teaming, Pilot deployments
- Utilization: Open Sourcing, Licensing, New Companies, Adoption by cyber operations analysts, Direct private-sector adoption, Government use

Implement Presidential Memorandum

- *"Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses" (Oct 28, 2011)*

NOTE: This slide was converted from the original graphic to text only in order to meet 508 compliance. For the original graphic, contact Mary Hanson, mary.hanson@hq.dhs.gov

Homeland Security
Science and Technology

Cyber-Physical Systems

- PPD 21 Identifies critical infrastructure as “interdependent functions and systems in both the physical space and cyberspace” and aims to strengthen security and resilience “against both the physical and cyber attacks”
- Cyber Physical Systems Are Becoming Ubiquitous:
  - Smart cars, smart grids, smart medical devices, smart manufacturing, smart homes, etc.
  - You will “bet your life” on many of these systems
  - Fast moving field focusing on functionality now and will bolt on security later…
- Transportation (Auto, UAVs, Aeronautical, Rail)
- Manufacturing
- Healthcare
- Energy
- Agriculture
- Emergency Response

Opportunity Now To Build Security Into Emerging Cyber Physical Designs

NOTE: This slide was converted from the original graphic to text only in order to meet 508 compliance. For the original graphic, contact Mary Hanson, mary.hanson@hq.dhs.gov

Homeland Security
Science and Technology

CSD New Programs / Ideas

- * *Security for Cloud-Based Systems*
- * *Data Privacy Technologies*
- * *Mobile Wireless Investigations*
- * *Mobile Device Security*
- * *Next-Generation DDOS Defenses*
- Application Security Threat Attack Modeling (ASTAM)
- Static Tool Analysis Modernization Project (STAMP)
- Network Reputation and Risk Analysis
- Data Analytics Methods for Cyber Security
- Cyber Security Education / Learning
- Designed-In Security
- Finance Sector Cybersecurity (14 topics)
- DNSSEC Applications
- Data Provenance for Cybersecurity
- Cyber Economic Incentives – based on EO/PPD

* *Approved*

Homeland Security
Science and Technology

2014 BAA Planning

- Anticipated Schedule
  - 15 Apr: BAA Pre-release to participating countries
  - 1 May: Pre-release of BAA Topic Calls – asking countries to commit resources – funding, governments reviewers
  - 15 May+: Publish BAA Topic Calls
    - Open to all respondents
  - June 2014 – March 2015: BAA White Paper and Proposal Review process and Contracting Activities

CSD R&D Execution Model

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

- First, critical infrastructure owners and operators and DHS customers develop prioritized requirements
- Then, RDTE&T occurs in three-stages: Pre-R&D (workshops and solicitations), R&D (program support) and Post-R&D (experiments and tech transfer)

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

Reference: "Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice," IEEE Security & Privacy, March-April 2013, Maughan, Douglas; Balenson, David; Lindqvist, Ulf; Tudor, Zachary (http://www.computer.org/portal/web/computingnow/securityandprivacy)

NOTE: This slide was converted from the original graphic to text only in order to meet 508 compliance. For the original graphic, contact Mary Hanson, mary.hanson@hq.dhs.gov

Homeland Security
Science and Technology

Summary

- Cybersecurity research is a key area of innovation to support our global economic and national security futures
- 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
- Need to continue strong emphasis on technology transfer and experimental deployments
- Must focus on the education, training, and awareness aspects of our current and future cybersecurity workforce

Homeland Security
Science and Technology

CSD Observations

- My thoughts on HSSTAC interactions with CSD:
- Frequency and quality of interactions
  - Over the past 6+ years, 4 interactions has been too few and future interactions should be much more frequent
  - Quality of interactions has been excellent; Help and support from HSSTAC has been beneficial
- Future Considerations
  - Knowledge of current HSSTAC members in Cybersecurity is insufficient
  - Suggest HSSTAC consider establishing topic-specific subcommittees or working groups to enable more and better technical interactions