DHS S&T Cybersecurity R&D Activities

Greg Wigton
Program Manager

Northeast Gas Executive Conference
September 8, 2014

http://www.dhs.gov/cyber-research
Speaker Background

- Schaefer Corporation – Contractor to DHS S&T (2005)
- DHS S&T (2006 – Present)
- Bachelor of Business, Management Information Systems (University of Notre Dame, 2003)
- MBA Candidate, Virginia Tech (2016)
Current Programs

- Critical Infrastructure
  - LOGIIC – Linking the Oil and Gas Industry to Improve Cybersecurity
  - TCIPG – Trustworthy Cyber Infrastructure for the Power Grid
- Cyber Exercise Technologies
- Enterprise Level Security Metrics
- Useable Security
Cyber Threat Sources Ready to Exploit Weaknesses

- **Cyber Criminals**
- **Nation States**
- **Terrorists, DTOs, etc.**
- **Hackers/Hacktivists**
- **Insider Threats**
Cyber Threats

- Malware – Malicious software to disrupt computers
- Viruses, worms, …
- Theft of Intellectual Property or Data
- Hactivism – Cyber protests that are socially or politically motivated
- Domain Name System (DNS) Hijacking
- Router Security – BGP Hijacking
- Denial of Service (DOS) – blocking access to web sites
- 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…)
- Supply Chain Vulnerabilities
- Others …..

**Bottom Line:** Easier to be a bad guy and volume of threats is growing
DHS provides advice and alerts to the 16 critical infrastructure areas ...

... DHS collaborates with sectors through Sector Coordinating Councils (SCC)
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
In February 2013, the President issued two new policies:

1) Executive Order 13636: Improving Critical Infrastructure Cybersecurity


- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensible to reducing the risk to these vital systems
DHS Requirements - QHSR

- **Mission 4: Safeguarding and Securing Cyberspace**
- **Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment.** Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation’s information infrastructure.
  - Understand and prioritize cyber threats
  - Manage risks to cyberspace
  - Prevent cyber crime and other malicious uses of cyberspace
  - Develop a robust public-private cyber incident response capability

- **Goal 4.2 Promote Cybersecurity Knowledge and Innovation.** Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.
  - Enhance public awareness
  - Foster a dynamic workforce
  - Invest in innovative technologies, techniques, and procedures
Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure
- Enhance the exchange of information and intelligence on risks to critical infrastructure and develop real-time situational awareness capabilities that ensure machine and human interpretation and visualization;
- Partner with critical infrastructure owners and operators to ensure the delivery of essential services and functions;
- Identify and understand interdependencies and cascading impacts among critical infrastructure systems;
- Collaborate with agencies and the private sector to identify and develop effective cybersecurity policies and best practices; and
- Reduce vulnerabilities and promote resilient critical infrastructure design.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise
- Coordinate government purchasing of cyber technology to enhance cost-effectiveness;
- Equip civilian government networks with innovative cybersecurity tools and protections; and
- Ensure government-wide policy and standards are consistently and effectively implemented and measured.

Goal 4.3: Advance Law Enforcement, Incident Response, and Reporting Capabilities
- Respond to and assist in the recovery from cyber incidents; and
- Deter, disrupt, and investigate cybercrime.

Goal 4.4: Strengthen the Ecosystem
- Drive innovative and cost effective security products, services, and solutions throughout the cyber ecosystem;
- Conduct and transition research and development enabling trustworthy cyber infrastructure;
- Develop skilled cybersecurity professionals;
- Enhance public awareness and promote cybersecurity best practices; and
- Advance international engagement to promote capacity building, international standards, and cooperation.
**CSD Mission & Strategy**

**REQUIREMENTS**

- **CSD MISSION**
  - Develop and deliver new technologies, tools and techniques to defend and secure current and future systems and networks
  - Conduct and support technology transition efforts
  - Provide R&D leadership and coordination within the government, academia, private sector and international cybersecurity community

**CSD STRATEGY**

- Trustworthy Cyber Infrastructure
- Cybersecurity Research Infrastructure
- Network & System Security and Investigations
- Cyber Physical Systems
- Transition and Outreach
"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

Successes
Over 30 products transitioned since 2004, including:

- 2004 – BAA 04-17
  - 5 commercial products
  - 2 Open Source products
- 2005 – BAA 05-10 (RTAP)
  - 1 commercial product
  - 1 GOTS product
  - 1 Open Source product
- 2007 – BAA 07-09
  - 2 commercial products
- 2011 – BAA 11-02 (more to come)
  - 1 Open Source product
  - 1 Research Infrastructure
- Law Enforcement Support
  - 2 commercial products
  - 1 Open Source product
  - Multiple Knowledge products
- Identity Management
  - 1 Open Source standard and GOTS solution
- SBIRs
  - 8 commercial products
  - 1 Open Source product
Cyber Security Budget Overview

![Budget Overview Chart]

The chart above illustrates the growth in the cyber security budget from Fiscal Year 2003 (FY03) to FY2015. The budget has significantly increased from FY03 to FY15, reaching its peak in FY15.
Objective: Develop standards, policies, processes, and technologies to enable more secure and robust global cyber infrastructure and to identify components of greatest need of protection, applying analysis capabilities to predict and respond to cyber attack effects and provide situational understanding to providers.

Secure Protocols
Develop agreed-upon global infrastructure standards and solutions
Working with IETF standards, routing vendors, global registries and ISPs
Provide global Routing Public Key Infrastructure (RPKI) solutions
Follow same process used for DNSSEC global deployment

Internet Measurement and Attack Modeling (IMAM)
Create more complete view of the geographical and topological mapping of networks and systems
Improve global peering, geo-location, and router level maps to assist automated solutions for attack prevention, detection, response
Support cross-org, situational understanding at multiple time scales

Distributed Denial of Service Defenses (DDOSD)
- Policy-based technologies to shift the advantage to the defender
- Measurement/analysis tools to test success of BCP38 deployments
- Engaging with major finance sector companies and supporting ISPs
Network and System Security and Investigations - 1

Objective: Develop new and innovative methods, services, and capabilities for the security of future networks and systems to ensure they are usable and security properties can be measured and provide the tools and techniques needed for combatting cybercrime.

Security for Cloud-Based Systems
Develop methodologies and technologies for cloud auditing and forensics in end-point devices.
Identify data audit methodologies to identify the location, movement, and behavior of data and Virtual Machines (VMs).
Work with DHS CIO/CISOs and datacenters.

Mobile Device Security
Develop new approaches to mobile device security (user identity/authentication, device management, App security and management, and secure data) for government purposes.
Working with DHS CISO and across several components.

Identity Management / Data Privacy
Advance the identity management ecosystem to support Federal, state, local, and private sector identity management functions.
Develop data privacy technologies to better express, protect, and control the confidentiality of private information.
Working with DHS, other Federal, State, Local and Private Sector.
**Objective:** Develop new and innovative methods, services, and capabilities for the security of future networks and systems to ensure they are usable and security properties can be measured and provide the tools and techniques needed for combatting cybercrime

**Software Quality Assurance**
Develop new methods and capabilities to analyze software and address the presence of internal flaws and vulnerabilities to reduce the risk and cost associated with software failures
Develop automated capability to bring together independent software and system assessment activities

**Usable Security and Security Metrics**
Improve the usability of cybersecurity technologies while maintaining security
Develop security metrics and tools and techniques to make them practical and useful as decision aids for enterprise security posture

**Investigation Capabilities for Law Enforcement**
Develop investigative tools/techniques for LE agencies to address the use of computers/phones in criminal and cyber related crimes
Develop techniques and tools focused on detecting and limiting malicious behavior by untrustworthy insiders inside an organization
Cyber Forensics Working Group – USSS, ICE, CBP, FBI, S/L
Objective: Ensure necessary security enhancements are added to the design and implementation of ubiquitous cyber physical systems and process control systems, with an emphasis on transportation, emergency response, energy, and oil and gas systems.

Cyber Physical Systems Security (CPSSEC)
- Build security into the design of critical, smart, networked systems
- Gain better understanding of threats and system interactions
- Testing and validation of solutions in partnership with private sector
- Working with DoTrans and NPPD and Transportation Sector

Trustworthy Computing Infrastructure for the Power Grid (TCIPG)
- Improve the security of next-generation power grid infrastructure, making the underlying infrastructure more secure, reliable and safe
- 4 University consortium – UIUC, WSU, UC-Davis, Dartmouth
- Private sector advisory board provides reqmts and transition path
- Partnership with DOE ($12M); Planning joint FY15 recompete

Securing the Oil and Gas Infrastructure (LOGIIC)
- Conduct collaborative RDT&E to identify and address sector-wide vulnerabilities in oil and gas industry digital control systems
- All R&D projects identified and funded by private sector members
- CSD provides project mgmt. support and inter-sector support
Objective: Develop research infrastructure, such as test facilities, realistic datasets, tools, and methodologies to enable global cybersecurity R&D community researchers to perform at-scale experimentation on their emerging technologies with respect to system performance goals

Experimental Research Testbed (DETER)
- Researcher and vendor-neutral experimental infrastructure
- Used by 300+ organizations from 25+ states and 30+ countries - DARPA
- Used in 40 + classes, from 30 institutions and 3,000+ students
- Open Source code used by Canada, Israel, Australia, Singapore

Research Data Repository (PREDICT)
- Repository of over 700TB of network data for use by community
- More than 250 users (academia, industry, gov’t – NSA SBIR)
- Leading activities on ICT Research Ethics (e.g., Menlo Report)
- Opening up to international partners (JP, CA, AU, UK, IL, EU)

Software Assurance Market Place (SWAMP)
- A software assurance testing and evaluation facility and services
- Advance the quality and usage of SwA tools – commercial & open
- IOC – 2/1/14; 500+ assessments/week; 8 platforms; 5 SwA tools
Objective: Accelerate the transition of mature federally-funded cybersecurity R&D technology into widespread operational deployment; Educate and train the current and next generations of cybersecurity workforce through multiple methods, models, and activities

Transition To Practice (TTP)
- White House initiated program; CSD budget plus-up in FY12
- Working with DOE and DOD labs, FFRDCs, UARCs, NSF, SBIRs
- Developing relationships in the Energy and Finance Sectors
- Multiple pilots in progress; Two commercial licensing deals done

Cybersecurity Competitions
- Provide a controlled, competitive environment to assess a student’s understanding and operational competency
- CSD-funded technologies included for test and evaluation
- 180+ schools and 1500+ college students participated in 2014
- Involvement from private sector; Assisting int’l competitions

National Initiative for Cybersecurity Education (NICE)
Joint DHS/NSF/DOD/DOEd initiative with WH and NIST support
Enhance Awareness (led by NPPD); Expand the Pipeline (led by CSD, NSF, DOEd); Evolve the Profession (led by NPPD and DOD)
- National Academic Consortiums – FY14 solicitation thru NIST
Education: A National Problem

- **Enhance public awareness**: (1) Augment current messaging to promote policies and practices that support Administration priorities, such as EO 13636 and PPD-21, and (2) develop messaging that targets senior executives of critical infrastructure companies (e.g., CEOs, Boards of Directors).

- **Expand the Pipeline**: (1) Expand formal education at the post-secondary level, including both four-year and two-year institutions and (2) establish new National Academic Consortia for Cybersecurity Education (government, colleges/universities, high schools, middle schools, technical academies, industry, professional organizations).

- **Evolve the profession**: (1) Identify critical cybersecurity workforce skills through a national cybersecurity Workforce Inventory and Gap Analysis and continued development of Cybersecurity Workforce Forecasting Tools and (2) provide access to free or low-cost training for the identified critical skills.
Transition To Practice (TTP) Program

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
CSD Projects / Relationships

People
- Secure Protocols
- Identity Management
- Enterprise Level Security Metrics
- Usable Security
- Data Privacy
- Cyber Forensics
- Competitions – Education
- Mobile Device Security
- Insider Threat

Systems
- Process Control Systems (PCS)
- Internet Measurement & Attack Modeling
- Cyber Physical Systems
- Distributed Denial of Service (DDoS) Defenses

Infrastructure
- Secure Protocols

Research Infrastructure
- Experimental Research Testbed (DETER)
- Research Data Repository (PREDICT)
- Software Quality Assurance (SWAMP)

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

- Software Quality Assurance
- Homeland Open Security Technology
- Assessments & Evaluations
- Experiments & Pilots
S&T International Engagements

- **International Bilateral Agreements**
  - Government-to-government cooperative activities for 13 bilateral Agreements
    - Canada (2004)
    - Australia (2004)
    - United Kingdom (2005)
    - Singapore (2007)
    - Sweden (2007)
    - Mexico (2008)
    - Israel (2008)
    - France (2008)
    - Germany (2009)
    - New Zealand (2010)
    - European Commission (2010)
    - Spain (2011)
    - Netherlands (2013)

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>PROJECTS</th>
<th>MONEY IN</th>
<th>MONEY OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>3</td>
<td>$300K</td>
<td>$400K</td>
</tr>
<tr>
<td>Canada</td>
<td>11</td>
<td>$1.8M</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
<td>$300K</td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td>2</td>
<td>$100K</td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>7</td>
<td>$450K</td>
<td>$1.2M</td>
</tr>
<tr>
<td>Sweden</td>
<td>4</td>
<td>$650K</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>3</td>
<td>$1.0M</td>
<td>$400K</td>
</tr>
<tr>
<td>European Union</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Over $6M of International co-funding
2014 Broad Agency Announcement

- **Anticipated Schedule**
  - 23 Apr: BAA released incl. to participating countries
    - $95M over 5 year period
  - S&T BAA Website: [https://baa2.st.dhs.gov](https://baa2.st.dhs.gov)
  - 1 June+: Publish BAA Topic Calls
    - Open to all respondents – foreign and domestic
  - June 2014 – March 2015: BAA White Paper and Proposal Review process and Contracting Activities

International Collaborations

![Flag Images]
### 2014 BAA – Topics

<table>
<thead>
<tr>
<th>Data Privacy:</th>
<th>CPSSEC:</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://go.usa.gov/8JZ9">http://go.usa.gov/8JZ9</a></td>
<td><a href="http://go.usa.gov/8JBQ">http://go.usa.gov/8JBQ</a></td>
</tr>
<tr>
<td>- TTA #1 - Privacy Policy Compliance Tools</td>
<td>- TTA #1 - Security Models and Interactions</td>
</tr>
<tr>
<td>- TTA #2 - Privacy-Preserving Federated Search</td>
<td>- TTA #2 - Secure System Design and Implementation</td>
</tr>
<tr>
<td>- TTA #3 - Mobile Computing Privacy</td>
<td>- TTA #3 - Experiments and Pilots</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile Tech Sec:</th>
<th>DDoSD:</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://go.usa.gov/8JBY">http://go.usa.gov/8JBY</a></td>
<td><a href="http://go.usa.gov/8JBB">http://go.usa.gov/8JBB</a></td>
</tr>
<tr>
<td>- TTA #1 - Mobile Device Instrumentation</td>
<td>- TTA #1 - Measurement &amp; Analysis to Promote Best Current Practices (BCP 38, SAC004)</td>
</tr>
<tr>
<td>- TTA #2 - Transactional Security Methods</td>
<td>- TTA #2 - Tools for Communication and Collaboration</td>
</tr>
<tr>
<td>- TTA #3 - Mobile Security Mgmt Tools</td>
<td>- TTA #3 - Novel DDoS Attack Mitigation and Defense Techniques</td>
</tr>
<tr>
<td>- TTA #4 - Protecting Mobile Device Layers</td>
<td></td>
</tr>
</tbody>
</table>
Important program for creating new innovation and accelerating transition into the marketplace

Since 2004, DHS S&T Cyber Security has had:
- 74 Phase I efforts
- 28 Phase II efforts
- 4 Phase II efforts currently in progress
- 10 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

S&T BAA / SBIR Website: https://baa2.st.dhs.gov
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 (2)
- Solid State Drive Analysis (1)
FY13
- Hybrid Analysis Mapping
- Software Based Roots of Trust for Enhanced Mobile Device Security
FY14
- Embedded System Security
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
LOGIIC – Operational Context

DHS S&T

- Program Management
- Subject Matter Expertise
- Access to Labs
- Testing Facilities
- Independent Researchers

ISA Automation Federation (AF)
(Legal Framework)

Oil & Gas Sector
Participating Companies

- Project #1
- Project #2
- Project #3
- Project #4
- Project #N

Findings

Outreach
- CI Owners and Operators
- Industry
- Vendors
- Standards Bodies

Current Members

$\$
TCIPG – Operational Context

DHS S&T
Cyber Security Expertise

DOE
Power Expertise

External Advisory Committee
(8 Members)

Outreach
Publications
Seminars & Webcasts
Vendors
Operators
Education

Industry Interaction Board
SIEMENS
GE
Sandia National Laboratories
NERC
Honeywell
Entergy
Cisco Systems
EPRI

TCIPG Research
(University of Illinois, Dartmouth College, Cornell University, University of California at Davis, Washington State University)

Technologies
Tools
Applications

Industry
Vendors
Operators
Standards

Transition

$ $ $
MOU between DHS S&T, NIST, and FS Sector Coord Council (FSSCC) in coordination with WH

Framework for public-private collaboration on R&D projects for the FS

Initial projects
- High Assurance Domains (e.g., DNSSEC)
- Identity Management
Why Partnerships?

- Cybersecurity impacts everyone
- Leverage the expertise of multiple groups
- Information sharing
- Lessons learned
- Raise the bar for everyone
Summary / Conclusions

- Cybersecurity research is a key area of innovation to support our global economic and national security futures.

- CSD continues with an aggressive cyber security research agenda to solve the cyber security problems of our current and future infrastructure and systems.
  - Particular challenges include scope/complexity of the different areas of the problem, and the balance of near versus longer-term R&D.

- Will continue strong emphasis on technology transition.

- Will impact cyber education, training, and awareness of our current and future cybersecurity workforce.

- Will continue to work internationally to find the best ideas and solutions to real-world problems.
Greg Wigton
Program Manager
Cyber Security Division
Homeland Security Advanced Research Projects Agency (HSARPA)
Gregory.Wigton@dhs.gov
202-254-6140

For more information, visit
http://www.dhs.gov/cyber-research
http://www.dhs.gov/st-csd