

# DHS S&T Cyber Security R&D Program

RDX Workshop  
Ottawa, Canada  
September 21, 2006



***Douglas Maughan, Ph.D.***  
***Program Manager, HSARPA***  
***[douglas.maughan@dhs.gov](mailto:douglas.maughan@dhs.gov)***  
***202-254-6145 / 202-360-3170***



**Homeland  
Security**

# Science and Technology (S&T) Mission

---



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



**Homeland  
Security**

# HSARPA Mission

---



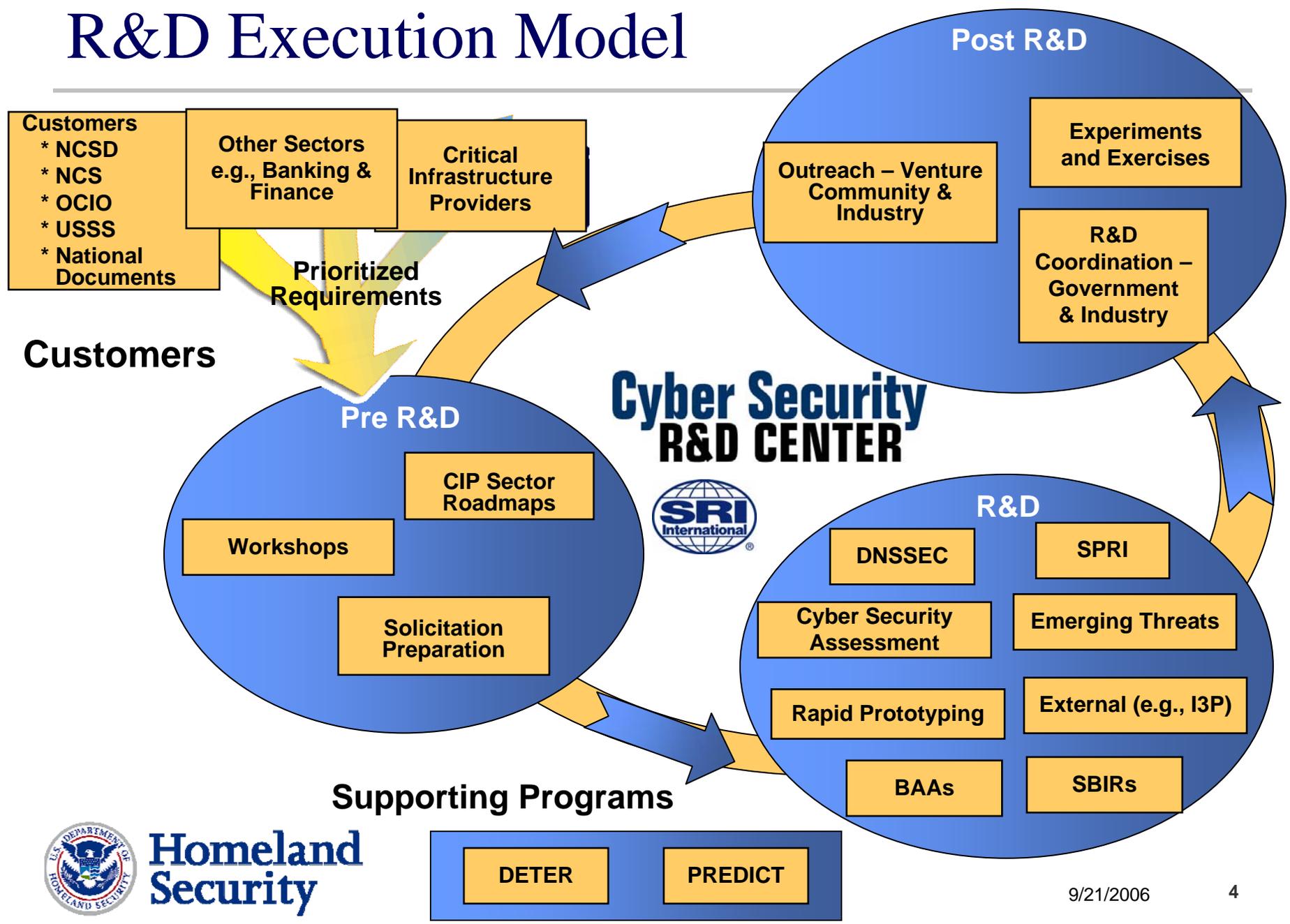
Engage **the Private Sector** in R&D to satisfy homeland security needs

- Satisfy operational requirements
- Conduct rapid prototyping and commercial adaptation
- Research & develop revolutionary options



**Homeland  
Security**

# R&D Execution Model



**Homeland Security**

# Cyber Security Program Areas

---

- 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
- Other Activities (SBIR, RTAP, I3P, Emerging Threats, ITTC, Outreach)



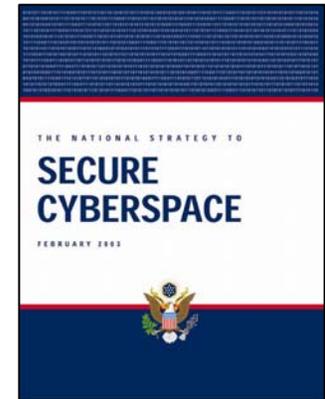
# Information Infrastructure Security (IIS)



# Information Infrastructure Security Motivation

---

- The National Strategy to Secure Cyberspace (2003) recognized the DNS and BGP as critical weaknesses of the Internet infrastructure
  - ◆ NSSC called for the Department of Homeland Security to coordinate public-private partnerships to encourage the adoption of improved security protocols, such as DNSSEC and Secure BGP
  - ◆ **The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS.** The Nation has a vital interest in ensuring that this work proceeds. **The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.**



# DNSSEC Initiative Activities

---

- Roadmap published in February 2005
  - ◆ <http://www.dnssec-deployment.org/roadmap.php>
- Multiple workshops held world-wide (ICANN, IETF, RIRs)
- DNSSEC testbed developed at NIST
  - ◆ <http://www-x.antd.nist.gov/dnssec/>
- Involvement with numerous deployment pilots
- Publicity and awareness plan – DNSSEC Newsletter
- Working with U.S. Civilian government (.gov) to develop policy and technical guidance for secure DNS operations and beginning deployment activities at all levels.
- Working with the operators of the “.us” and “.mil” zones towards DNSSEC deployment and compliance

# Secure Protocols for the Routing Infrastructure (SPRI)

---

- BGP is the routing protocol that connects ISPs and subscriber networks together to form the Internet
- BGP does not forward subscriber traffic, but it determines the paths subscriber traffic follows
- The BGP architecture makes it highly vulnerable to human errors and malicious attacks against
  - ◆ Links between routers
  - ◆ The routers themselves
  - ◆ Management stations that control routers
- Work with industry to develop solutions for our current routing security problems and future technologies



# SPRI Way Ahead

---

- Working with ARIN to clean up existing database and legacy address space problem
  - ◆ Pre-1997 IP Addresses are not accounted for
- Working with ARIN and APNIC to deploy PKI between ICANN/IANA and registry and between registry and ISPs/customers
- Working with ISPs to identify remaining R&D and necessary tools for secure routing management

# Cyber Security Research Tools and Techniques (RTT)



# DHS / NSF Cyber Security Testbed

---

- **“Justification and Requirements for a National DDOS Defense Technology Evaluation Facility”, July 2002**
- We still lack large-scale deployment of security technology sufficient to protect our vital infrastructures
  - ◆ Recent investment in research on cyber security technologies by government agencies (NSF, DARPA, armed services) and industry.
- One important reason is the lack of an experimental infrastructure and rigorous scientific methodologies for developing and testing next-generation defensive cyber security technology
- The goal is to create, operate, and support a researcher-and-vendor-neutral experimental infrastructure that is open to a wide community of users and produce scientifically rigorous testing frameworks and methodologies to support the development and demonstration of next-generation cyber defense technologies



# DETER Experimenters Community

## User Organizations

---

- Bell Labs
- Boeing Phantom Works
- Columbia University
- Cs3 Inc.
- Dalhousie University
- Federated Investors
- Flux Group, University of Utah
- George Mason University
- HP Labs
- ICSI / LBNL
- Information Sciences Institute
- IntruGuard Devices, Inc.
- Juniper
- Lehigh University
- McAfee Research
- National Cyber-Forensics and Training Alliance
- Naval Postgraduate School
- Network Associates Laboratories
- New Jersey Institute of Technology
- Penn State University
- Princeton University
- Purdue University
- Rutgers University
- Sandia National Laboratories
- Secure64 Software Corp
- SPARTA, Inc.
- SRI International
- Telcordia Technologies
- Technical University Berlin
- The SANS Institute
- UC Berkeley
- UC Davis
- UC Irvine
- UC Santa Cruz
- UC San Diego
- Univ. of North Carolina at Charlotte
- University of Delaware
- University of Illinois, Urbana-Champaign
- University of Maryland
- University of Texas at Austin
- Warrior LLC
- Washington University in St. Louis
- Western Michigan University



**Homeland  
Security**

# A Protected REpository for Defense of Infrastructure against Cyber Threats

---

- PREDICT Program Objective
  - “To advance the state of the research and commercial development (of network security ‘products’) we need to produce datasets for information security testing and evaluation of maturing networking technologies.”
- Rationale / Background / Historical:
  - ◆ Researchers with insufficient access to data unable to adequately test their research prototypes
  - ◆ Government technology decision-makers with no data to evaluate competing “products”

**End Goal: Improve the quality of defensive cyber security technologies**



**Homeland  
Security**

# Data Collection Activities

---

- Classes of data that are interesting, people want collected, and seem reasonable to collect
  - ◆ Netflow
  - ◆ Packet traces – headers and full packet (context dependent)
  - ◆ Critical infrastructure – BGP and DNS data
  - ◆ Topology data
  - ◆ IDS / firewall logs
  - ◆ Performance data
  - ◆ Network management data (i.e., SNMP)
  - ◆ VoIP (1400 IP-phone network)
  - ◆ Blackhole Monitor traffic

# Experiments and Exercises

---

- Experiments
  - ◆ U.S. / Canada Secure Blackberry Experiment
    - PSTP-agreed upon deployment activity
  - ◆ Oil and Gas Sector
    - Working with industry, labs, researchers, and vendors
  - ◆ Department of Treasury
    - FS ISAC, FSSCC, Numerous sector participants
- Exercises
  - ◆ National Cyber Security Exercise (Cyber Storm)
    - DETER Testbed

# US-CAN Secure Wireless Trial

- Objective

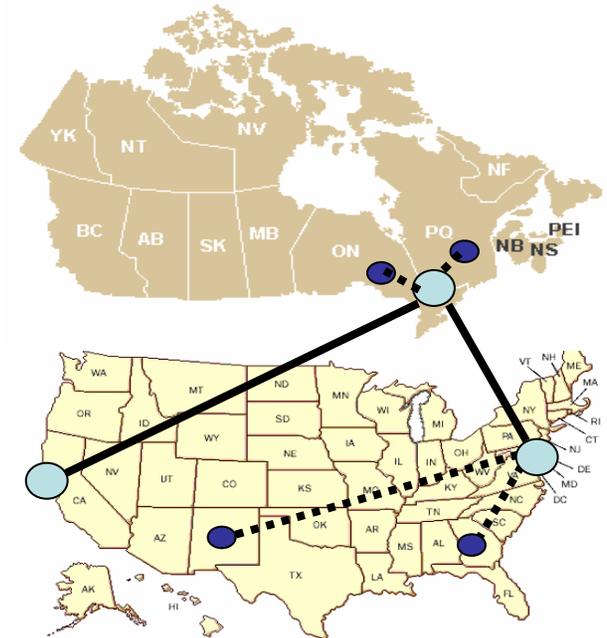
- ◆ Test effectiveness of US/Canadian cross-border secure wireless architecture to cope with real-time communication in variety of scenarios

- Technologies

- ◆ PKI (S/MIME), Identity-based encryption, enforcement of policy and compliance

- Trial Activity

- ◆ July 2005: U.S.-only initial four-day test period
- ◆ October 2005: Four-day test period with 35 activities and with 40+ participants acting out homeland security scenarios using BlackBerry devices



# LOGIIC™ Partnership

Project LOGIIC is a model for government-industry technology integration and demonstration efforts to address critical R&D needs

- Industry contributes
  - ◆ Requirements and operational expertise
  - ◆ Project management
  - ◆ Product vendor channels
- DHS S&T contributes
  - ◆ National Security Perspective on threats
  - ◆ Access to long term security research
  - ◆ Independent researchers with technical expertise
  - ◆ Testing facilities



**Homeland  
Security**



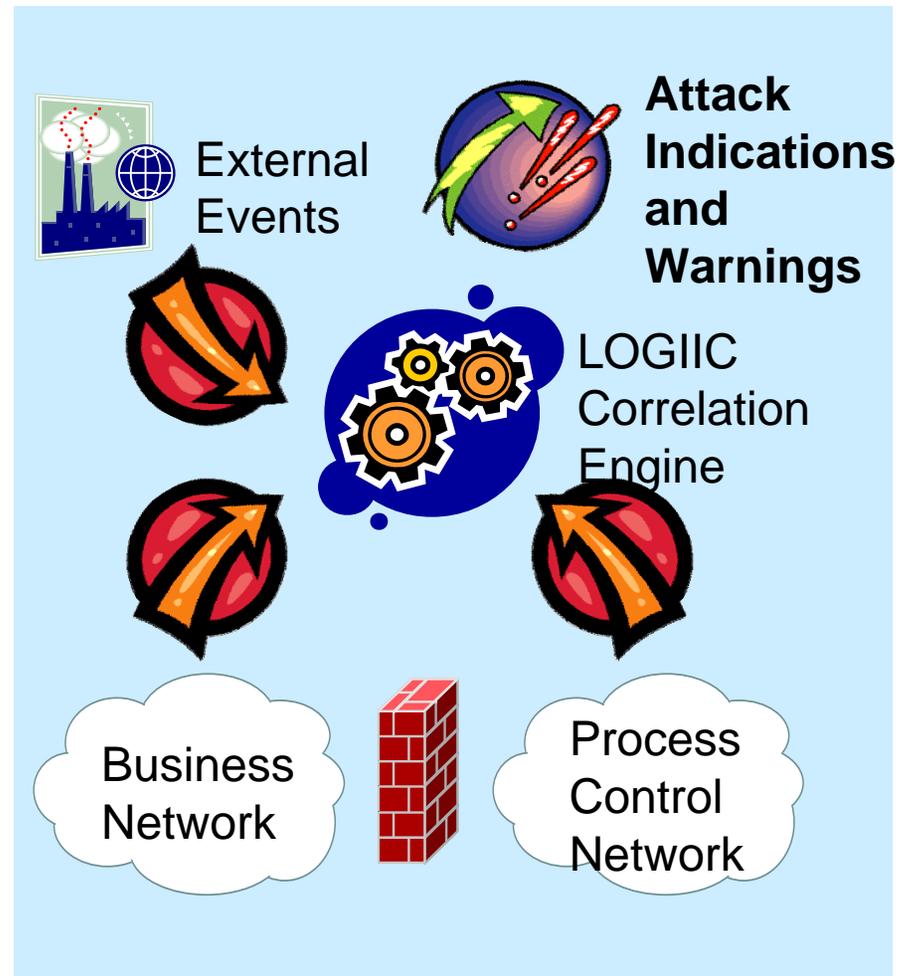
**ERGON**



**Sandia  
National  
Laboratories**

# LOGIC™ Overview

- Opportunity: Reduce vulnerabilities of oil & gas process control environments by correlating and analyzing abnormal events to identify and prevent cyber security threats
- Approach:
  - ◆ Identify new types of security sensors for process control networks
  - ◆ Adapt a best-of-breed correlation engine to this environment
  - ◆ Integrate in testbed and demonstrate
  - ◆ Transfer technology to industry



**Homeland  
Security**

# Next Generation Cyber Security Technologies (NGT)



# HSARPA Cyber Security Broad Area Announcement (BAA 04-17)

---

- The goals of the Cyber Security Research and Development (CSRD) program are:
  - ◆ 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 develop new and enhanced technologies for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure.
  - ◆ To facilitate the transfer of these technologies into the national infrastructure as a matter of urgency.
- **<http://www.hsarpabaa.com>**



**Homeland  
Security**

# BAA Technical Topic Areas (TTAs)

---

- System Security Engineering
  - ◆ Vulnerability Prevention
  - ◆ Vulnerability Discovery and Remediation
  - ◆ Cyber Security Assessment (i.e., Metrics)
- Security of Operational Systems
  - ◆ Security and Trustworthiness for Critical Infrastructure Protection
  - ◆ Wireless Security
- Investigative and Prevention Technologies
  - ◆ Network Attack Forensics (e.g., Traceback)
  - ◆ Technologies to Defend against Identity Theft

# 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



## Other Activities:

SBIR

RTAP

I3P

Emerging Threats

ITTC

Outreach

R&D Coordination



**Homeland  
Security**

# Small Business Innovative Research (SBIR)

---

- FY04
  - ◆ Cross-Domain Attack Correlation Technologies
  - ◆ Real-Time Malicious Code Identification
- FY05
  - ◆ Hardware-assisted System Security Monitoring
- FY06
  - ◆ Network-based Boundary Controllers
  - ◆ Botnet Detection and Mitigation

# Rapid Technology Application Program (RTAP) - Cyber Security Topics

---

- BOTNET Detection and Mitigation Tool
  - ◆ Customer: NCSD
- Exercise Scenario Modeling Tool
  - ◆ Customer: NCSD
- DHS Secure Wireless Access Prototype
  - ◆ Customer: S&T OCIO



# The Institute for Information Infrastructure Protection (I3P)

---

- The I3P is a consortium of 30 academic and not-for-profit research organizations
  - ◆ The I3P was formed in September 2001 and funded by congressionally appropriated funds assigned to Dartmouth College (\$17.8M)
- Two major research programs
  - ◆ Process Control (PCS) and Supervisory Control and Data Acquisition (SCADA) systems
  - ◆ Economic and policy issues associated with cyber security deployment



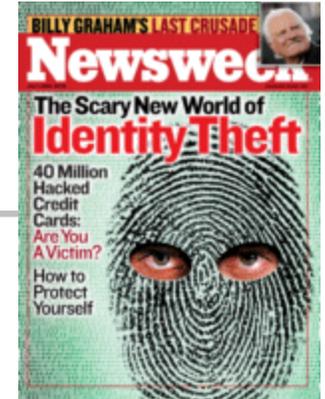
# Emerging Threats

---

- Virtual Machine Environment - Detection and Escape Prevention
  - ◆ Vulnerability Discovery and Defenses for Virtual Machines
- Next Generation Crimeware Defenses
  - ◆ Research new techniques for defending against next generation malicious software
- Botnet Command & Control Detection and Mitigation
  - ◆ Examine defenses needed to counter new methods of Botnet C&C



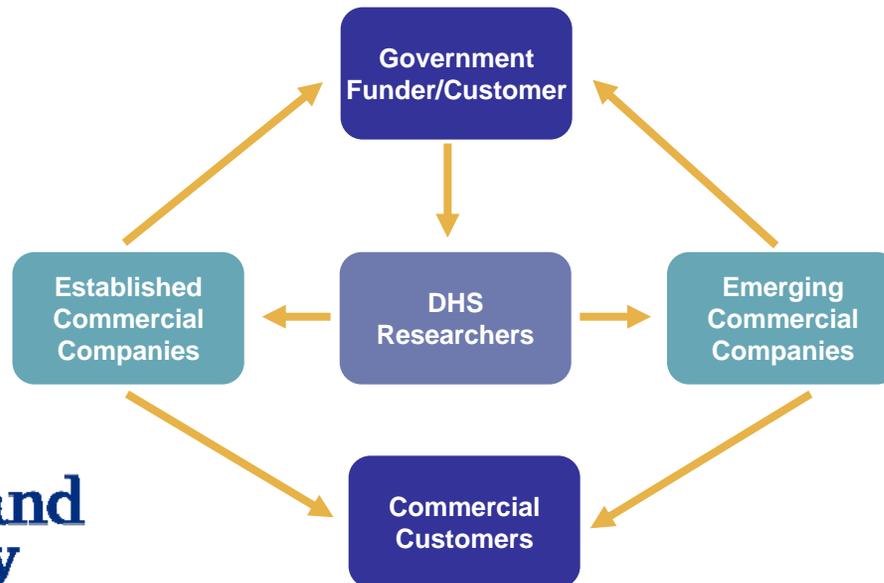
# ITTC – The DHS-SRI Identity Theft Technology Council



- ITTC is an expanded Silicon Valley expert group originally convened by the U.S. Secret Service
- Experts and leaders from
  - ◆ Government
  - ◆ Financial and IT sectors
  - ◆ Venture capital
  - ◆ Academia and science
- ITTC works closely with The Anti-Phishing Working Group (APWG)  
  
<http://www.anti-phishing.org>
- ITTC Coordinator: Robert Rodriguez, retired head of the Secret Service Field Office in San Francisco
- The ITTC was formed in April 2005, and has four active working groups:
  - ◆ Reports / Studies
    - Phishing Technology
    - Crimeware
  - ◆ Data collection and sharing
  - ◆ Future threats
  - ◆ Development and deployment

# Commercial Outreach Strategy

- Assist commercial companies in providing technology to DHS and other government agencies
  - ◆ Emerging Security Technology Forum (ESTF)
- Assist DHS S&T-funded researchers in transferring technology to larger, established security technology companies
  - ◆ DHS Mentor / Protégé program, System Integrator Forum
- Partner with the venture capital community to transfer technology to existing portfolio companies, or to create new ventures



# Tackling Cyber Security R&D Challenges: *Not* Business as Usual

---

- Strong mission focus (avoid mission creep)
- Close coordination with other Federal agencies
- Outreach to communities outside of the Federal government
  - ◆ Building public-private partnerships (the industry-government \*dance\* is a new tango)
- Strong emphasis on technology diffusion and technology transfer
- Migration paths to a more secure infrastructure
- Awareness of economic realities

# Summary

---

- DHS S&T is moving forward with an aggressive cyber security research agenda
- Working with the community to solve the cyber security problems of our current infrastructure
  - ◆ DNSSEC, Secure Routing
- Working with academe and industry to improve research tools and datasets
  - ◆ DHS/NSF Cyber Security Testbed, PREDICT
- Looking at future RDT&E agendas with the most impact for the nation
  - ◆ BAA 04-17, SBIRs, RTAP, Emerging Threats

---

***Douglas Maughan, Ph.D.***  
***Program Manager, HSARPA***  
**[douglas.maughan@dhs.gov](mailto:douglas.maughan@dhs.gov)**  
***202-254-6145 / 202-360-3170***

For more information, visit  
**<http://www.cyber.st.dhs.gov>**



**Homeland  
Security**