Cyber Security Research and Development: A Homeland Security Perspective

CERIAS Information Security Symposium

March 23, 2004

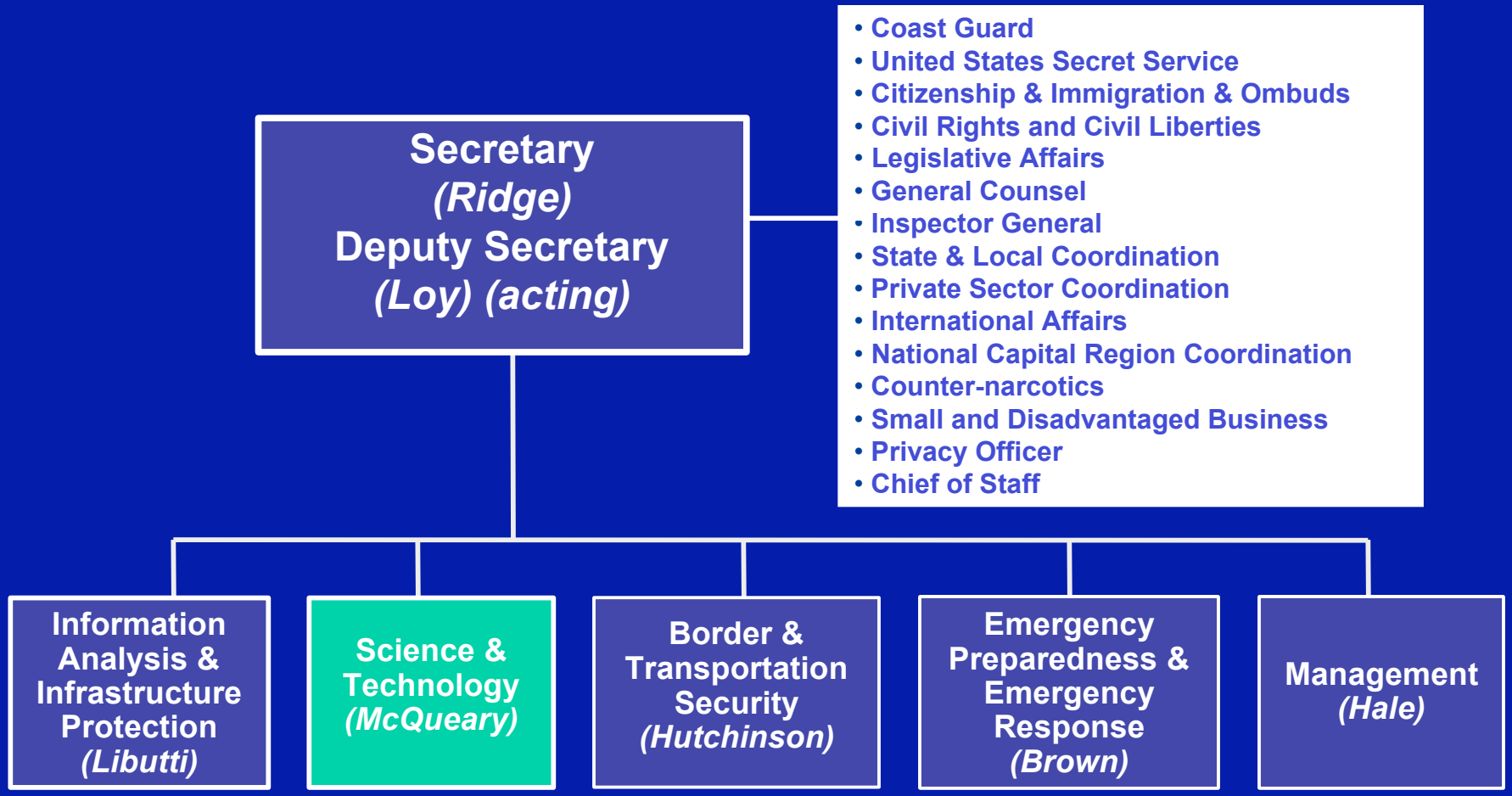
Simon Szykman, Ph.D.
Director, Cyber Security R&D
202-772-9867
simon.szykman@dhs.gov

Homeland Security

Outline

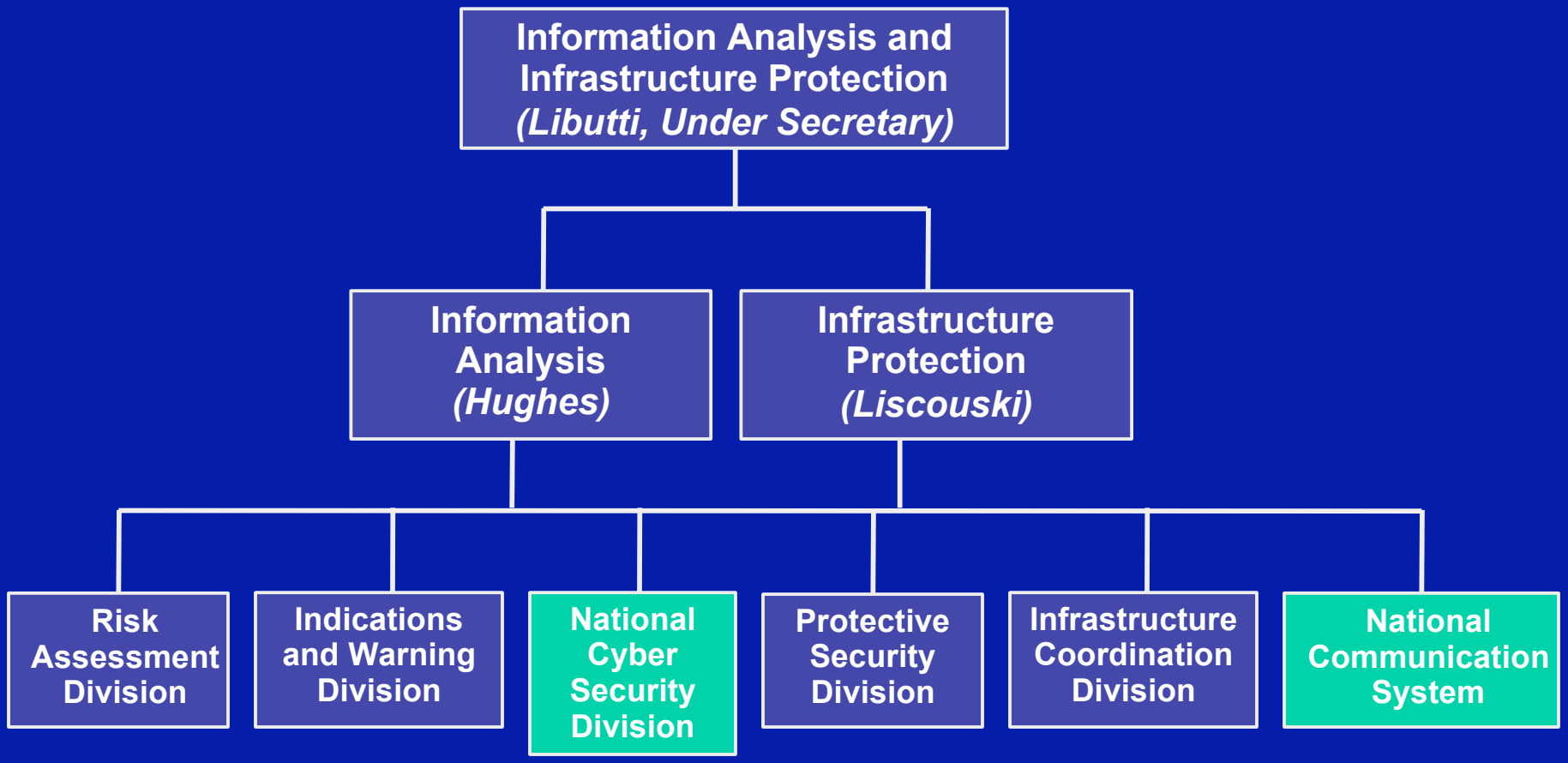
- DHS Organizational Overview
  - Cyber Security Stakeholders in DHS
- Science and Technology
- Office of University Programs
- DHS Cyber Security Research and Development
  - Research Interests and Priorities
  - DHS Challenges
- Challenges and Opportunities for Higher Education

Department of Homeland Security Overview



Homeland Security

Information Analysis and Infrastructure Protection Directorate



National Cyber Security Division Mission

The National Cyber Security Division (NCSD) is the national focal point for addressing cyber security issues in the United States and will coordinate implementation of the *National Strategy to Secure Cyberspace*.

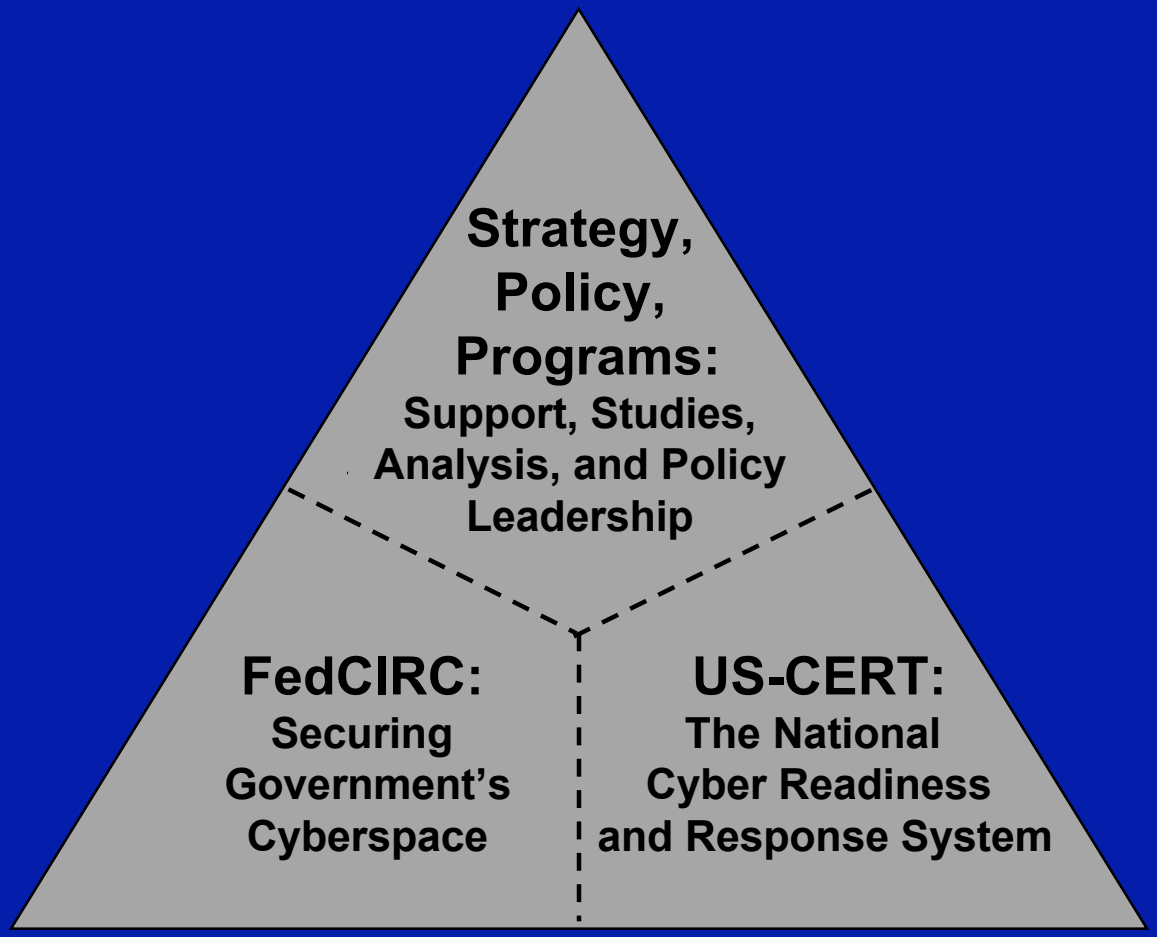
Mission components include:

1. Identifying, analyzing, and reducing threats and vulnerabilities
2. Disseminating threat and warning information
3. Coordinating incident response
4. Providing technical assistance in continuity of operations and recovery
5. Serving as national focal point for the public and private sectors regarding cyber security issues

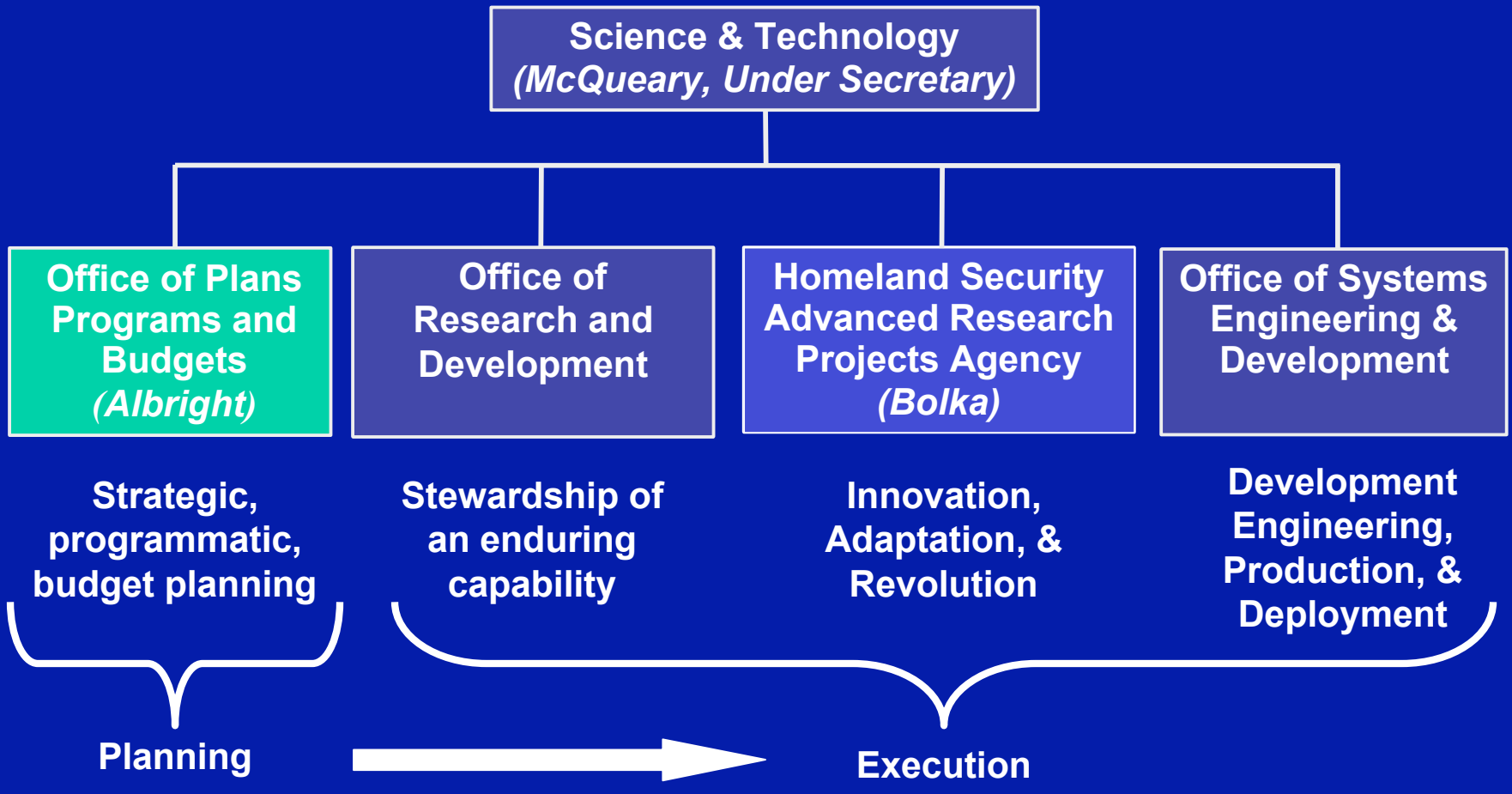
…to implement the National Cyber Strategy…

Homeland Security

NCSD's Integrated Capability



Science and Technology Directorate



Homeland Security

S&T Mission

- The US Department of Homeland Security's Science and Technology division:

Serves as the primary research and development arm of the Department, utilizing our nation's scientific and technological resources to provide federal, state, and local officials with the technologies and capabilities necessary to protect the homeland.

Homeland Security

S&T Responsibilities: Homeland Security Act of 2002

- Advising the Secretary regarding...
- Identifying priorities for…
- Establishing, conducting, and coordinating…

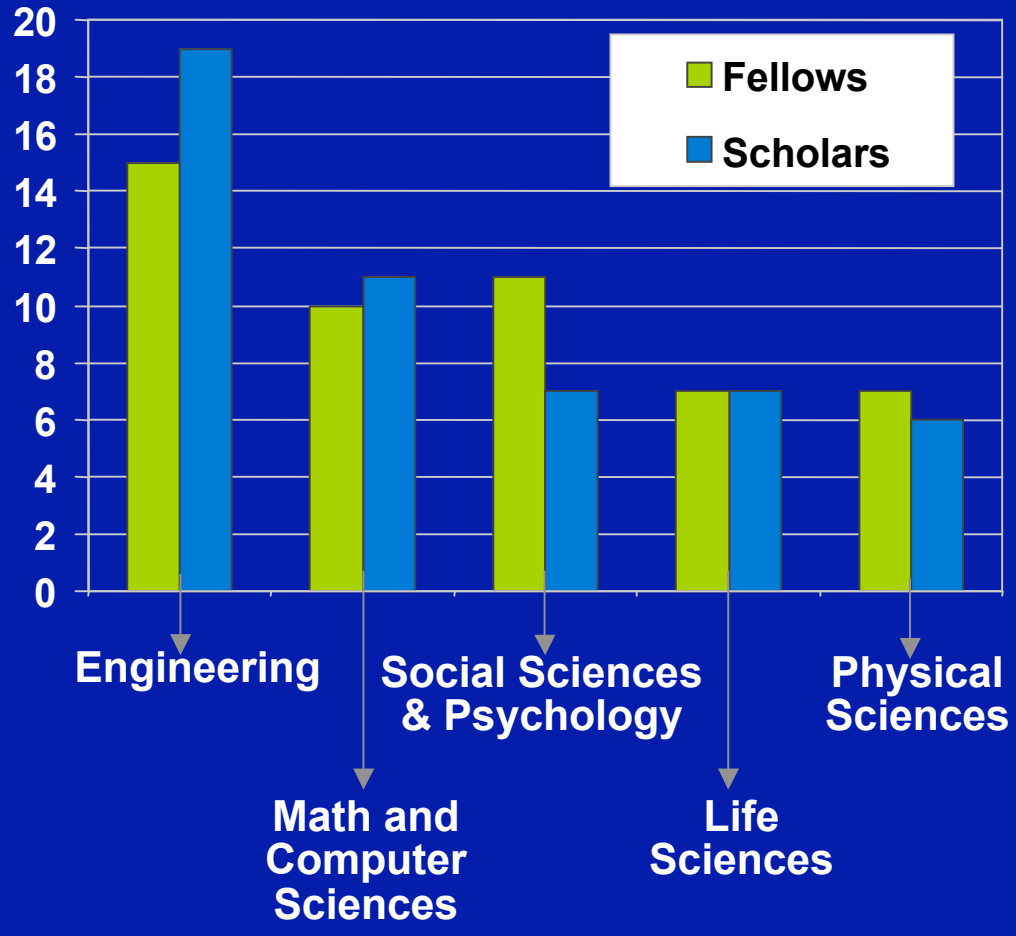
…basic and applied research, development, testing and evaluation (RDT&E) activities that are relevant to any or all elements of the Department, through both intramural and extramural programs.

HS Academic Centers of Excellence

- Recent award: Homeland Security Center for Risk and Economic Analysis of Terrorist Events
- Recent Broad Agency Announcement: Agro-terrorism countermeasures (animal disease, food contamination)
  - 25 proposals received by 2/9/04; awards in April
- Others under consideration
  - Behavioral research on terrorism and countermeasures
  - Public perceptions and responses to terrorism
  - Response technologies and operations
  - System deployment & information management of sensor networks

Homeland Security Scholars & Fellows

- 2003 Class
  - 50 Scholars and 50 Fellows in engineering, math, computer science, social sciences, life and physical sciences
- 2004 Class (2/19)
  - New competition
  - Quality internships
  - Alumni network
  - Post-doctoral program



Cyber Corps Program

- Scholarships for service program
  - University fellowships in return for working for the Federal government for two years after graduation.
- Capacity building track
  - Provides funds to university for development of faculty, programs and curricula in the area of cyber security.

Cyber Security R&D Portfolio: Scope

- The Internet serves a significant underlying role in many of the Nation's critical infrastructures.
  - Communications, monitoring, operations and business systems.
- Adversaries face asymmetric offensive and defensive capabilities with respect to traditional warfare.
  - Makes cyberspace is an appealing battleground.
- Cyberspace provides the ability to exploit weaknesses in our critical infrastructures.
  - Provides a fulcrum for leveraging physical attacks.

Cyber Security R&D Portfolio: Threats

- The most significant cyber threats to the nation are fundamentally different from the “script-kiddies” or virus writers.
- Adversaries who seek to harm the Nation’s critical infrastructure are driven by different motivations.
- DHS S&T focus is on those threats and issues that warrant national-level concerns.

Important R&D Areas

Securing the Infrastructure
- Secure domain name system
- Secure routing protocols
- Secure process control systems (retrofit and future infrastructure)

Cyber Security Functional Requirements
- Protection and prevention
- Situational awareness, incident & warning
- Detection and response
- Code development testing & analysis tools
- Authentication
- Forensics, traceback attribution
- Hardware/firmware security
- Secure operating Systems

Domain-Specific Security Needs
- Wireless
- Distributed & embedded, computing platforms

Other Needs
- Privacy
- Red teaming

Decision Support
- Metrics and testing
- Economic assessment
- Long term goal of risk-based decision making

Enabling Technologies for R&D
- Testbeds
- Modeling and simulation
- Network mapping
- Security technology and policy management

Homeland Security

Cyber Security R&D Portfolio: Overview

- FY 2004 cyber security R&D budget: $18M

  FY 2005 budget request: $18M
- Programs:
  - Next-Generation Cyber Security Technologies Program
  - Cyber Security Technology Infrastructure Program
  - Cyber Security Studies Program
  - Cyber Security Cooperative Research Communities Program
  - Cyber Security Small Development Projects Program
  - Cyber Security Small Business Innovation Research Program

Initial Research Priorities

- Securing infrastructural protocols:
  - Secure Domain Name System (DNSSEC) and Secure Border Gateway Protocol (BGP)
- Large-scale data sets for security testing
  - Essential for supporting development of cyber security metrics
- Economic assessment activities
  - Along with metrics, will provide a foundation for risk-based cyber security decision making
- Execution of top priorities from IAIP Directorate

Setting the Government Research Agenda

- Homeland Security Presidential Directive 7
  - National Science and Technology Council, Critical Information Infrastructure Protection Interagency Working Group
- InfoSec Research Council (IRC)
  - Revisiting the IRC Hard Problems List

Business *Not* as Usual

- Strong mission focus (avoid mission creep).
- Strong emphasis on technology diffusion.
- Close coordination with other Federal agencies.
- Supporting public-private partnerships.
- Maintain and enhance understanding of non-technical issues that affect cyber security.
- DHS S&T maintaining cooperative relationship with Congress.

DHS Challenges

- Creating effective public-private partnerships.
- Catalyzing cooperation among private sector competitors.
- Getting critical infrastructure sectors to secure their infrastructures.
- Migration to a more secure Internet.
- Technology transfer from government-funded R&D into commercial use.
- Economic realities.

Higher Education Community: Challenges

- Heterogeneous IT environments.
- Not traditionally oriented toward security.
- Appropriate tradeoff between security and openness.
- Security policy, controls, and enforcement.

Higher Education Community: Opportunities

- Strength in research
  - Source of new ideas and technology
  - Research centers (such as CERIAS) provide critical mass and generally emphasize partnerships with industry.
- Openness
  - Information sharing
- Freedom, and less prone to being risk averse
  - Can stay at the forefront of new technological developments
  - Pilot projects
- Organizing to function like a “sector”
  - Tailored standards, guidelines, and best practices

Questions?

Homeland Security

Simon Szykman, Ph.D.
Director, Cyber Security R&D
202-772-9867
simon.szykman@dhs.gov