Cyber Security Research and Development at the Department of Homeland Security

Briefing to the President's Information Technology Advisory Committee (PITAC)

April 13, 2004

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

Homeland Security

Outline

- Organizational Overview
- DHS Cyber Security Research and Development
  - Research interests and priorities
  - Ongoing and future activities
  - Perspectives on OSTP charge to PITAC

Department of Homeland Security Overview

Secretary
(Ridge)
Deputy Secretary
(Loy) (acting)

- Coast Guard
- United States Secret Service
- Citizenship & Immigration & Ombuds
- Civil Rights and Civil Liberties
- Legislative Affairs
- General Counsel
- Inspector General
- State & Local Coordination
- Private Sector Coordination
- International Affairs
- National Capital Region Coordination
- Counter-narcotics
- Small and Disadvantaged Business
- Privacy Officer
- Chief of Staff

Information Analysis & Infrastructure Protection ***(Libutti)***

Science & Technology ***(McQueary)***

Border & Transportation Security ***(Hutchinson)***

Emergency Preparedness & Emergency Response ***(Brown)***

Management ***(Hale)***

Homeland Security

Science and Technology Directorate

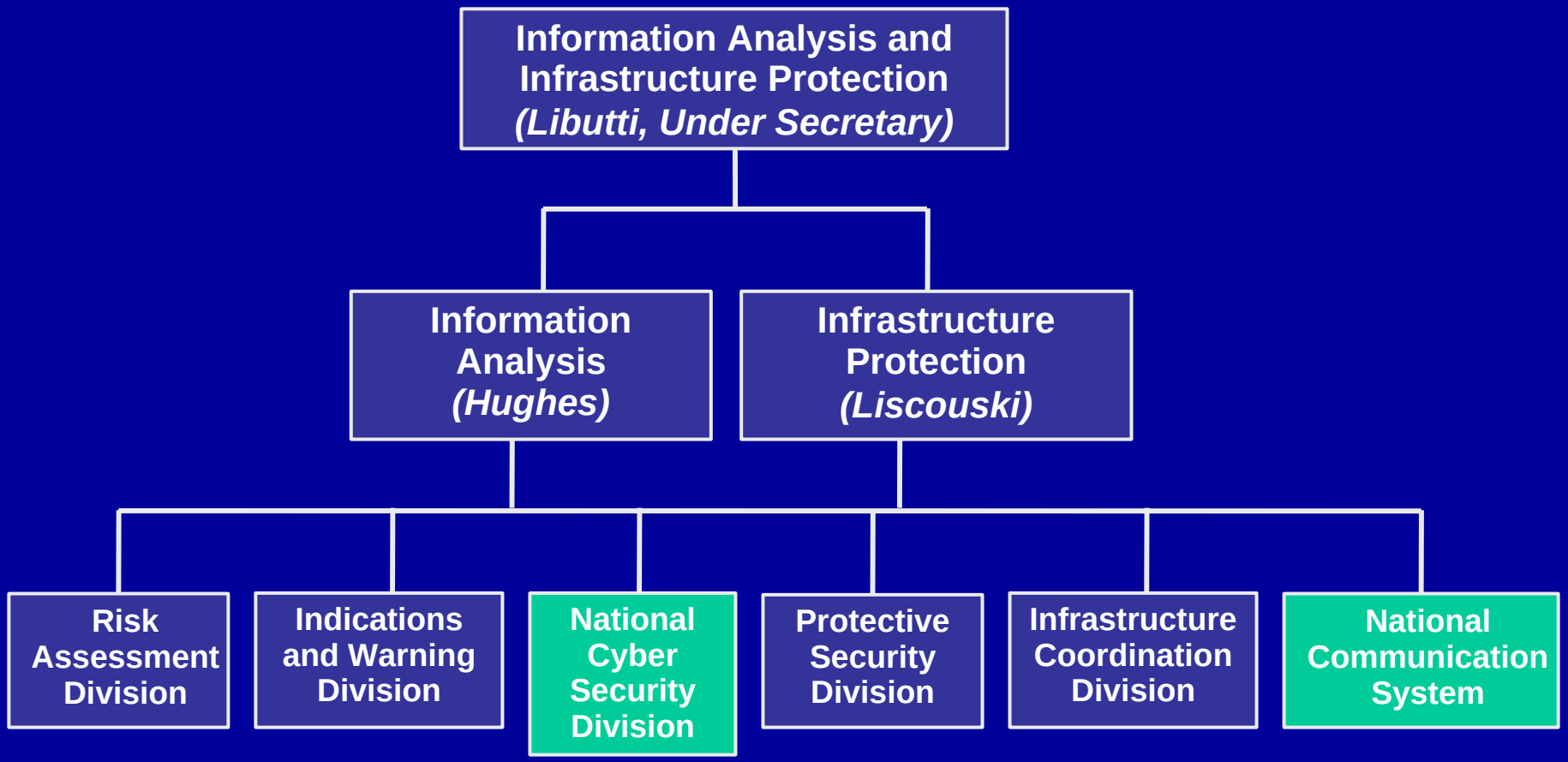
Science & Technology
(McQueary, Under Secretary)

Office of Plans Programs and Budgets *(Albright)*	Office of Research and Development	Homeland Security Advanced Research Projects Agency *(Bolka)*	Office of Systems Engineering & Development
Strategic, programmatic, budget planning	Stewardship of an enduring capability	Innovation, Adaptation, & Revolution	Development Engineering, Production, & Deployment

Planning → **Execution**

Homeland Security

Information Analysis and Infrastructure Protection Directorate



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.

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.

Questions put to PITAC by OSTP

- Is the government investing in the right areas? Balanced priorities among areas? Balanced priorities among low-risk and long-term research?

  ➔ In our view, this must be answered in the context of agency missions.

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
- Attack detection and response
- Secure code dev., code testing & analysis
- Lightweight, low-latency authentication
- Forensics, traceback attribution
- Hardware/firmware security
- Secure operating Systems

Domain-Specific Security Needs
- Wireless
- Internet Priority Service
- 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

Important R&D Areas

- Areas of interest include short, medium and long term needs. Initial priority is on:

1. Pressing customer needs:
   - Execution of top priorities from the Information Analysis and Infrastructure Protection Directorate
   - National Strategy to Secure Cyberspace
2. Foundations and infrastructure:
   - Economic assessment studies, large scale data sets for security testing
   - Securing infrastructural protocols (Domain Name System, Internet routing protocols, process control systems)

Questions put to PITAC by OSTP

- How well are efforts and institutions able to anticipate paradigm or technology shifts that can create unexpected cyber security challenges?

  ➔ Coordination of efforts across Federal agencies is a key.

Coordination of the Research Agenda

- National Science and Technology Council (NSTC) Critical Information Infrastructure Protection (CIIP) Interagency Working Group (IWG)
  - Responding to Homeland Security Presidential Directive 7
  - Maintaining ties with NSTC Networking and Information Technology Research and Development (NITRD) IWG
- InfoSec Research Council (IRC)
  - Revisiting the IRC Hard Problems List: 5-10 year problems that require sustained R&D investments

Questions put to PITAC by OSTP

- How effective have programs been in terms of successful outcomes and value of results?
- How useful have results been as measured by implementation to improve the Nation's security?

  ➔ DHS lacks a historical record on which to base evaluation of our programs

Effectiveness of DHS Programs

- Why do we believe we will be effective?
  - ➔ Strong management plan:
    - Defined mission
    - Eight strategic objectives identified for R&D portfolio
    - Long term vision (of which short term activities are a part)
    - Identified stakeholders (internal and external to DHS)
    - Alignment of activities with plan, objectives, customer requirements
    - Organization to support the above
    - Addressing broader set of challenges

Cyber Security R&D Center

- Virtual research and development center
  - Research performed by industry, universities, national labs…
- $3M technical, management, and administrative support contract awarded to SRI International

Pre-Research Activities:

- Sector roadmaps
- Workshops/meetings
- Research solicitations
- Proposal review

Post-Research Activities:

- Testbeds
- Experiments/exercises
- Venture capital community outreach
- Industry outreach
- Interface with non-government R&D communities

Addressing Broader set of Challenges

- Strong mission focus (avoid mission creep).
- Close coordination with other Federal agencies.
- Outreach to communities outside of the Federal government.
- Strong emphasis on technology diffusion and technology transfer.
- Migration to a more secure infrastructure.
- Awareness of economic realities.

Questions?

Homeland Security

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