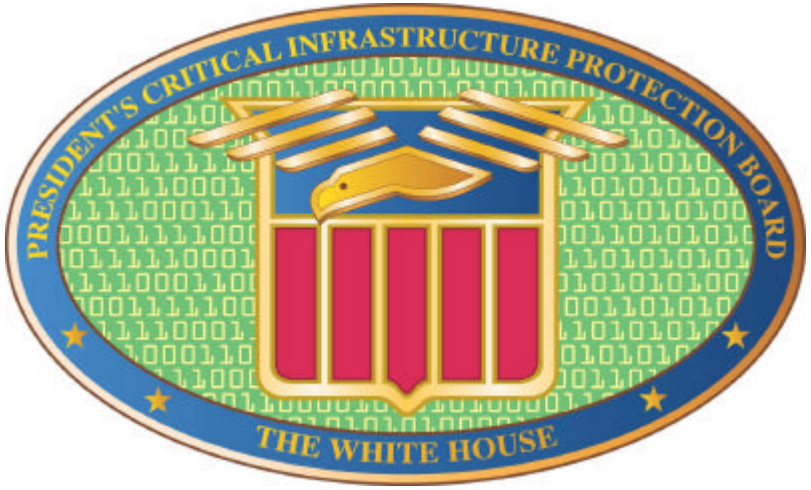
Boundaryless Information Flow: Keeping IT Secure

The National Strategy to Secure Cyberspace



February 3, 2003

Andy Purdy
Deputy to the Vice Chair
Senior Advisor, IT Security and Privacy
The President's Critical Infrastructure Protection Board
The White House

Overview

- **Information technology revolution has changed the way --**
  - **business is transacted,**
  - **government functions, and**
  - **national defense is conducted.**
- **Those three functions now depend on an interdependent network of information technology infrastructures**

The Case for Action

- **Protection of our information systems is essential to our critical infrastructures: telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services**

Overview

- **Cybersecurity is essential to ---**
  - **Our national security;**
  - **Our nation's economic well-being;**
  - **Law enforcement/public safety; and**
  - **Privacy.**
- **Our overall strategic goal is to empower all Americans to secure their portions of cyberspace.**

The Case for Action

- It is the policy of the United States to protect against disruptions of information systems for critical infrastructures
- Ensure disruptions are infrequent, minimal duration, manageable, cause least damage

Dangers
A Spectrum

- **Low end: teenage joyriders**
- **Up the spectrum: individuals engaged in ID theft, fraud, extortion, and industrial espionage**
- **Nations engaged in espionage against U.S. companies and U.S. government**
- **Far end: nations building information warfare units**

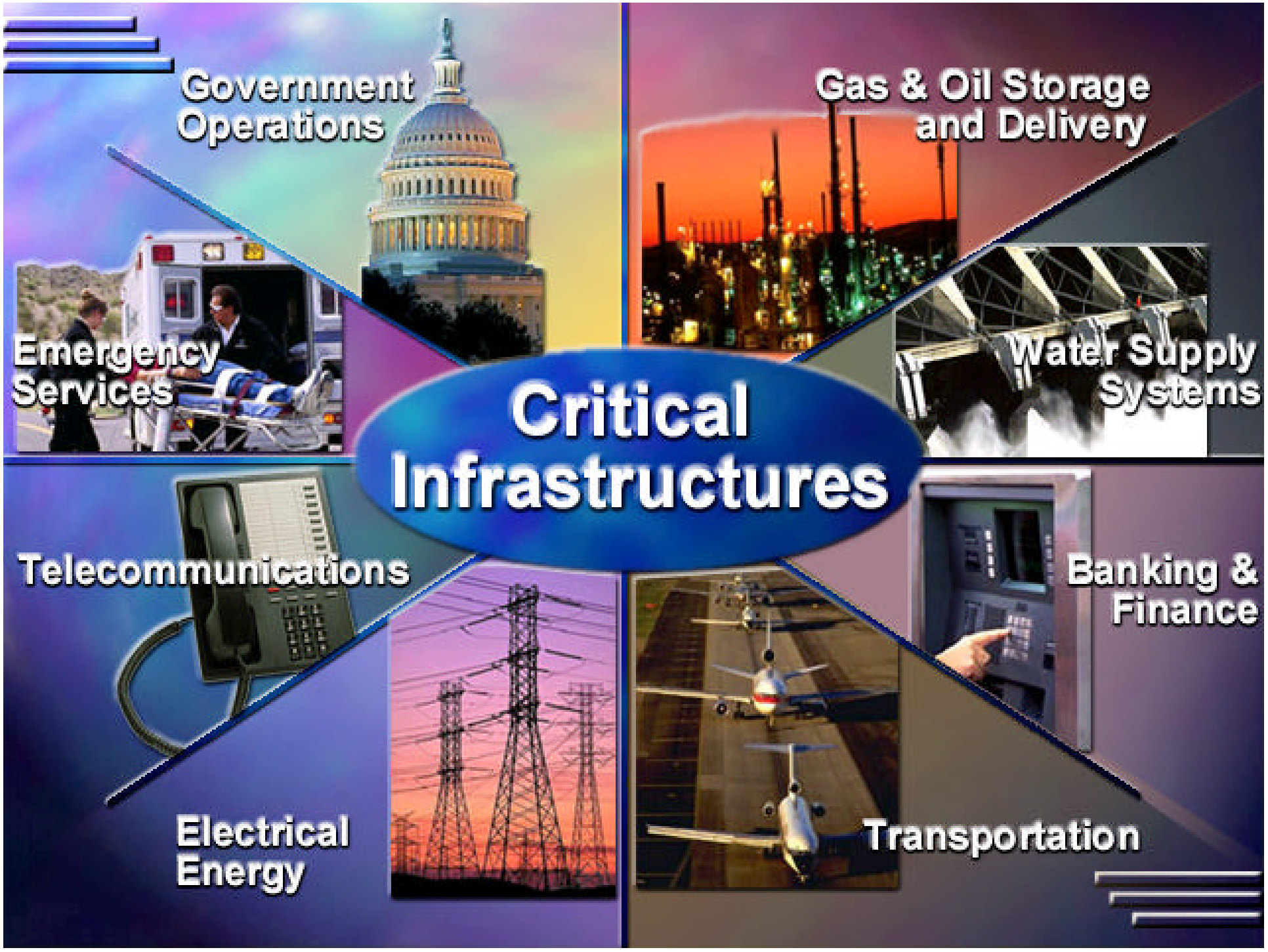
A New Paradigm

- **Stop focusing on specific threats**
- **Focus on vulnerabilities**

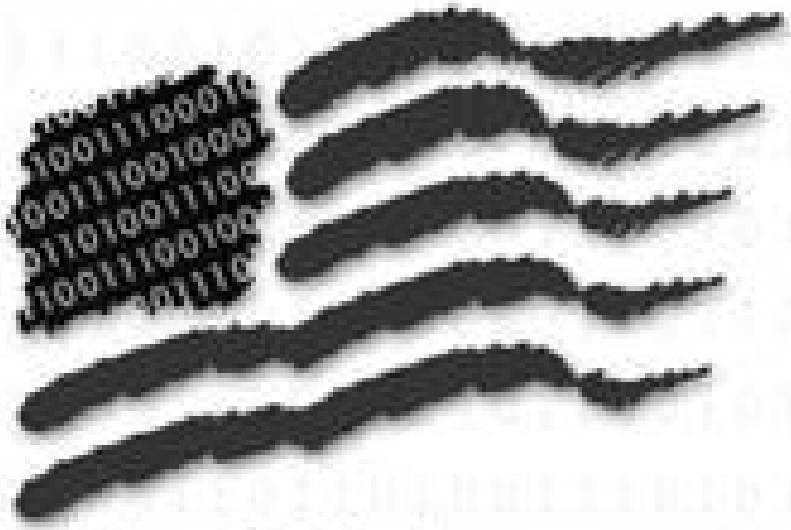
THE PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

Scope is directed by Executive Order 13231:

The protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.


Government Operations
Gas & Oil Storage and Delivery
Emergency Services
Water Supply Systems
Critical Infrastructures
Telecommunications
Banking & Finance
Electrical Energy
Transportation

The President's Critical Infrastructure Protection Board



THE NATIONAL STRATEGY TO SECURE CYBERSPACE

For Comment

SEPTEMBER 2002

DRAFT

A Strategy, Not a Plan

- Everyone is responsible for their portion of Cyberspace
- The Strategy provides a roadmap by
  - Removing barriers,
  - Empowering people and organizations to do their part, and
  - Fostering a national partnership between government, industry and individuals.

PRESIDENT'S
CRITICAL INFRASTRUCTURE
PROTECTION BOARD

What are the guiding principles of the Strategy?

- Encourage market forces to improve security, rather than using a regulatory approach
- Share information among and between companies, departments and agencies, and state/local govts.

PRESIDENT'S
CRITICAL INFRASTRUCTURE
PROTECTION BOARD

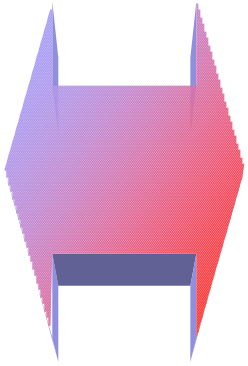
Guiding principles - continued

- Create public/private partnership solutions to IT security
- Clean up the Federal Government's own IT security problems as a model
- Foster public/ corporate awareness of importance of IT security

Strategy as Process

Government

- 53 Questions
  - Posted on multiple web sites
  - Published in media
- Town Halls in 4 cities
- Numerous interviews, speeches, media events



Non-Government

- Infrastructure sector plans
- 100's of pages of answers to questions
- Higher Education Strategy input

For sector strategies: www.pcis.org

National Strategy to Secure Cyberspace

- Home Users and Small Business
- Large Enterprises
- Sectors
  - Federal
  - State and Local
  - Higher Education
  - Private Industry
- National Priorities
- Global

Cyber R&D Priorities

Short Term (1-3 yrs)	**Enterprise wide automated security policy enforcement** **- Improvements in software patch management** **- Development and testing of protocols needed to secure the mechanisms of the Internet** **- Development and testing of security mechanisms for Supervisory Control and Data Acquisition (SCADA) Systems**

Cyber R&D Priorities

ShortTerm (1-3 yrs)	**- Development of secure operating Systems Expand the Institute for Information Infrastructure Protection's R&D agenda gap analysis program** **- Develop security enhancements for Ad hoc networks and grid computing**

Cyber R&D Priorities

Medium Term (3-5 yrs)

- Secure routers and switches and protocols
- Development of new protocols for Internet and wireless that maintain security at higher speeds and scales
- Investigation of the security implications of intelligent agent software in networks

Cyber R&D Priorities

Long Term (5-10 yrs)

- Fundamental shifts in technology and the development of novel or unforeseen applications, e.g., nano technology, quantum computing
- Provide a sound theoretical, scientific, and technological basis for assured construction of safe, secure systems
- Ultrasecure communications over optical backbone networks
- Orders of magnitude increases in the speed of algorithms such as for searching unsorted databases

Home Users/Small Business

- **Empower the home user and small business person to protect their cyberspace and prevent it from being used to attack others.**
- **Key Themes**
  - **You have a role in cyberspace security**
  - **You can help yourself**
  - **Promoting more secure Internet access**

Large Enterprise

- Encourage and empower large enterprises to establish secure systems.
- Key themes:
  - Raising the level of responsibility,
  - Creating corporate security councils for cyber security, where appropriate,
  - Implementing ACTIONS and best practices,
  - Addressing the challenges of the borderless network.

Critical Sectors

- **Specific sectors critical to cybersecurity, including:**
  - **Federal Government,**
  - **State/Local Governments,**
  - **Higher Education, and**
  - **Private sector**

Strategy as Process

Sectors Preparing Strategies

Electricity
North American Electrical Reliability Council

Oil & Gas
National Petroleum Council

Water
American Water Works Association

Transportation (Rail)
Association of American Railroads

Banking & Finance
Financial Services Round Table, BITS,

Information & Communications
Information Technology Association of America, Telecommunications Industry Association, United States Telecommunications Association Cellular Telecommunications and Internet Association,

- ***Chemicals*** *(Self-organized)*
- ***Education*** *(self-organized)*

What Has Changed

- Number of Recommendations
- Simplified structure to focus on 5 priorities
- Objectives parallel with NSHS:
  - **prevent cyber attacks;**
  - **reduce national vulnerabilities to cyber attacks; and**
  - **minimize the damage and recovery time from cyber attacks.**
- DHS actions prominent (consistent w/ legislation)
- More concise and decisive language

Strategy Outline

- Executive Summary
- Introduction
- Cyberspace Threats and Vulnerabilities: A Case for Action
- National Policy and Guiding Principles
- National Cyberspace Security Priorities
- Conclusion: The Way forward

THE PRESIDENT'S CRITICAL
INFRASTRUCTURE PROTECTION BOARD

What are some of the Board's Priorities?

1. Awareness: The National Cyber Security Alliance and its StaySafeonLine campaign
2. Education: The CyberCorps Scholarship for Service program
3. Info Sharing: The Cyber Warning & Info Network (CWIN) between Govt and Industry; limited FOIA exemption

THE PRESIDENT'S CRITICAL
INFRASTRUCTURE PROTECTION BOARD

Board's Priorities - Continued

4. Research: The CyberSecurity Research Consortium and a national research agenda

5. Protecting Internet Infrastructure: projects to secure Domain Name Servers and Border Gateway Protocols, blunt Distributed Denial of Service attacks

6. Physical Security of Key Nodes

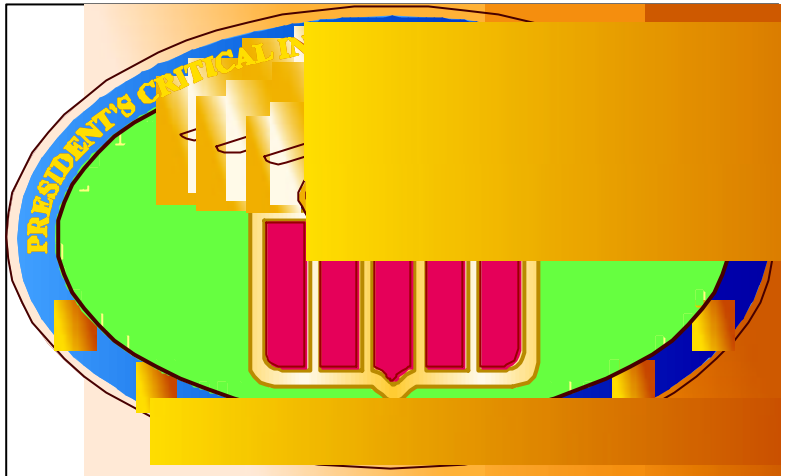
THE PRESIDENT'S CRITICAL
INFRASTRUCTURE PROTECTION BOARD

Board's Priorities - Continued

7. **Standard & Best Practices: including relating to Federal procurement**

8. **Digital Control Systems: securing utilities and manufacturing control systems**

9. **Securing Future Systems: beginning with new Wireless web enabled devices**



andy_purdy@nsc.eop.gov

Andy Purdy, 202-456-2821