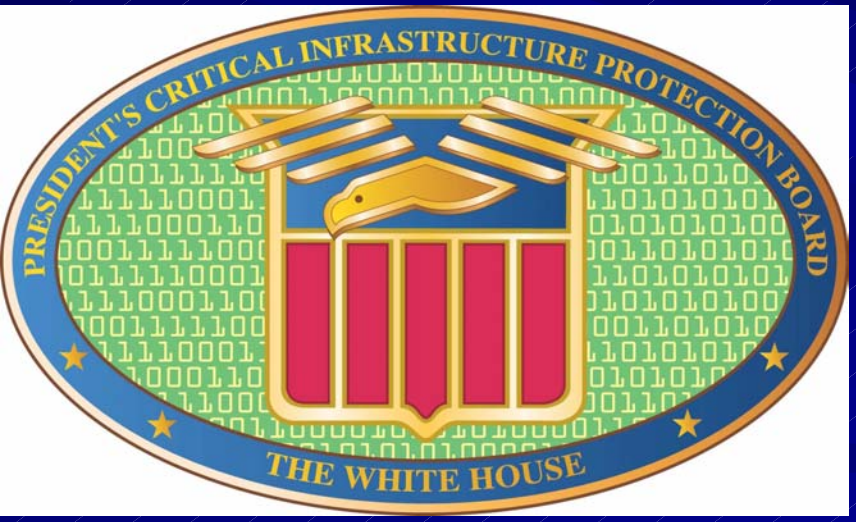
5th National HIPAA Summit

National Strategy to Secure Cyberspace

Privacy and Security in Healthcare



Andy Purdy
Senior Advisor, IT Security and Privacy
The President's Critical Infrastructure Protection Board
The White House

October 31, 2002

Foundation

- The nation's Strategy to Secure Cyberspace must be consistent with the core values of its open and democratic society.
- Americans expect government and industry to respect their privacy and protect it from abuse.
- This respect for privacy is a source of our strength as a nation.

OVERVIEW

- Lessons Learned from September 11
- The National Strategy to Secure Cyberspace
- Privacy and Security
- The Health Care Sector

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.

Learning Lessons from History

- Hindsight is not always 20/20
- We do not learn the same lesson
- Our memories are short

Lessons Learned

- We have enemies.
- Our enemies are smart.
- We must never underestimate them.

Lessons Learned

- We must be prepared for the likelihood that our enemies will use our technologies against us.
- Our enemies will find the seams, the holes, the weaknesses in our society…and they will exploit them to harm us.

Lessons Learned

- Our economic system is fragile … and far more interdependent than we realize.

Lessons Learned

- We need to work together to face the future.
- We need a public-private partnership the likes of which this nation has never seen.

Lessons Learned

- We must stop reasoning by analogy -- thinking that we have seen the worst case
- …that if it has not happened before it will not happen in the future.

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

The Case for Action

- 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

The Case for Action

- The Internet is at the core of the information infrastructure
- Internet was designed to easily share unclassified research among friends and colleagues; security not a concern
- Has grown increasingly insecure
- Around the globe people can access a network that is ultimately connected to networks that run critical functions in U.S.

The Case for Action
A Spectrum of Danger

- *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

The Case for Action

- Cyber attacks occur regularly and can have serious consequences, disrupting critical operations, causing loss of revenue and intellectual property
- 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

A New Paradigm

- Stop focusing on specific threats
- Focus on vulnerabilities

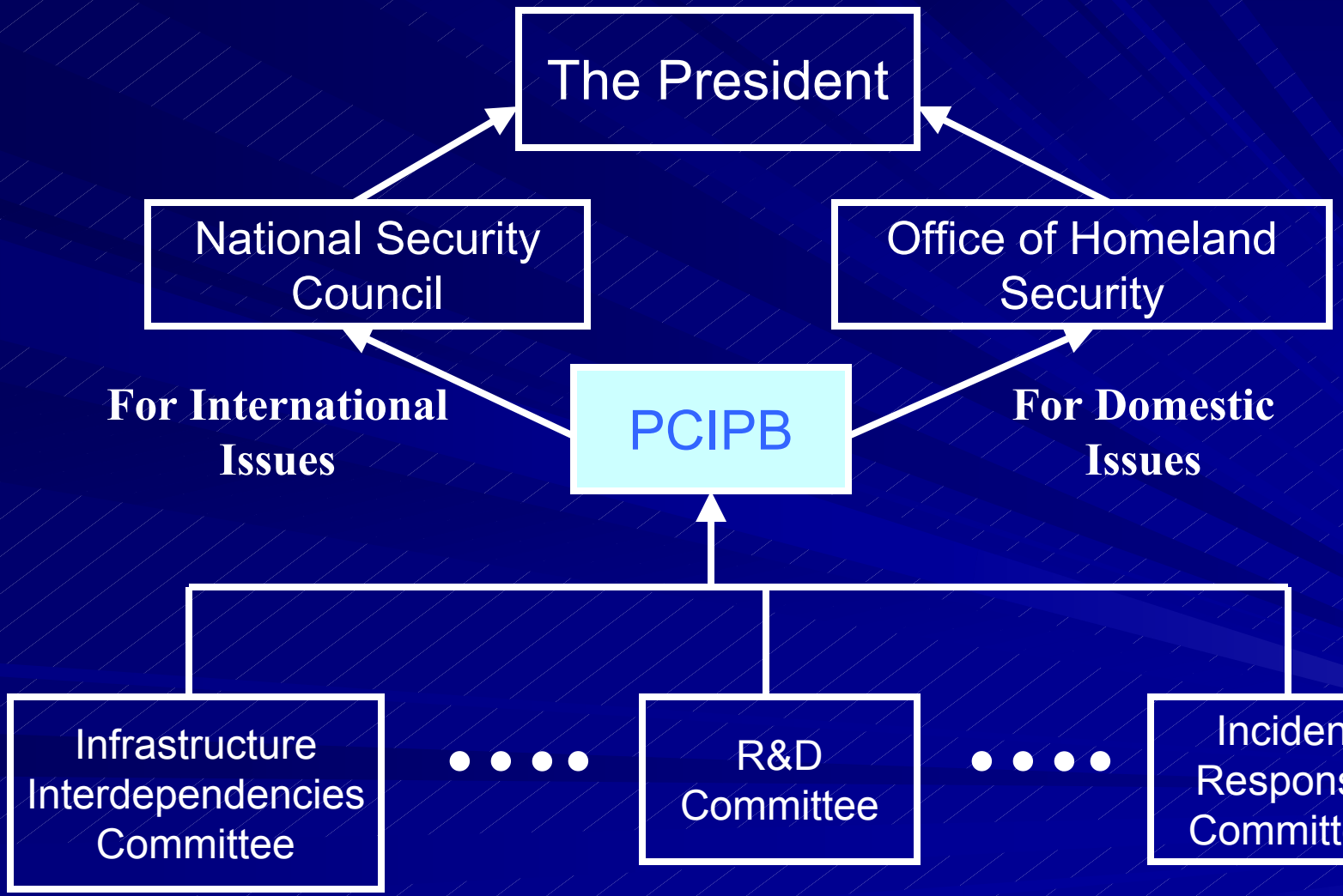
THE PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

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

Relationships



PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

What are the committees and who chairs them?

– Private Sector/State & Local Outreach	Commerce
– Executive Branch Info Systems Security	OMB
– National Security Systems	DOD
– Incident Response Coordination	FBI/DOD
– Research & Development	OSTP
– Infrastructure Interdependencies	OE/DOT

PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

Board committees - continued

– Finance and Banking	Treasury
– Education	NSA/DOA
– International Affairs	State
– Physical Security of Information Systems	DOJ/DOD
– National Security Emergency Preparedness Communications	DOD

PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

What are the guiding principles of the Board?

- 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

THE PRESIDENT'S CRITICAL
INFRASTRUCTURE PROTECTION BOARD

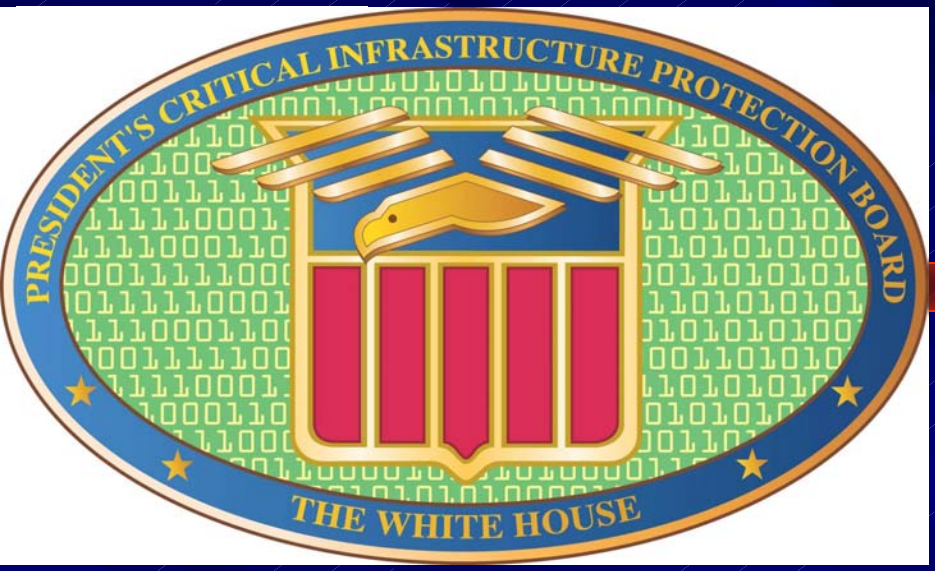
What is the Board doing?

The Board has been tasked by the President to create a National Strategy to Secure Cyberspace

--comments on September 18 draft due Nov. 18th

--a policy and programmatic road map for government and industry

--a modular strategy, on-line, adaptable to new threats and new technology



The National Strategy to Secure Cyberspace

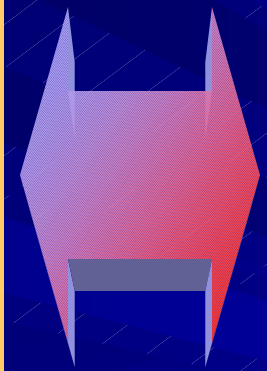
www.securecyberspace.gov

Comment due November 18

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

- Introduction
- Case for Action
- Policy and Principles
- Highlights
- Level 1: Home Users and Small Business
- Level 2: Large Enterprises

National Strategy to Secure Cyberspace

- Level 3: Sectors
  - Federal
  - State and Local
  - Higher Education
  - Private Industry
- Level 4: National Priorities
- Level 5: 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

Cyber R&D Priorities

Long Term (5-10 yrs)

- Ultrasecure communications over optical backbone networks
- Orders of magnitude increases in the speed of algorithms such as for searching unsorted databases

Level 1 – Home Users/ Small Business

- The strategic goal is to 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 (Links to get help)
  - Promoting more secure Internet access

Level 2
Large Enterprise

- The strategic goal is to 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.

Level 3
Critical Sectors

- Level 3 addresses 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)*

Level 4
National Priorities

Securing shared systems

- Securing the mechanisms of the Internet
- Digital Control Systems
- Research and development
- Highly secure and trustworthy computing
- Securing emerging systems
- Vulnerability remediation

Level 4
National Priorities

Fostering a reinforcing economic and social framework

- Awareness
- Training and education
- Certification
- Information sharing
- Cybercrime
- Market forces
- Privacy and civil liberties

Level 4
National Priorities

Developing national plans and policy

- Warning and analysis
- Continuity of operations, reconstitution and recovery
- National security
- Interdependency and Physical security

Level 5 - Global

- The strategic goal is to ensure the integrity of global information networks.
- Key themes:
  - Promote national and international watch and warning
  - Council of Europe Cybercrime Convention
  - North American "Cyber Safe Zone"
  - Cyber Points of Contact
  - Promote global "culture of security"

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

Privacy and Security

- The National Strategy must be consistent with the core values of our open and democratic society -- protecting privacy is fundamental.

Privacy and Security

- Explosion in information technology and the interconnectedness of information systems with the Internet raises legitimate concerns and challenges.
- We must ensure the integrity, reliability, availability, and confidentiality of data in cyberspace.

Privacy *and* Security

- **Privacy and security have common themes: stopping access, use, and disclosure of information.**
- **Good security should promote privacy protection by creating a record of access to information.**

Common Themes

- Identity and authority are critical
  - Identity theft
  - Financial records/access
  - Health records/access
- Need multiple verification - basic passwords are not sufficient

Privacy and Security

- Requires technology to facilitate fair information practices
  - Notice and awareness
  - Choice and consent
  - Access (by subject)
  - Information quality and integrity
  - Update and correction
  - Enforcement and recourse

Privacy Technology "The Privacy Framework"

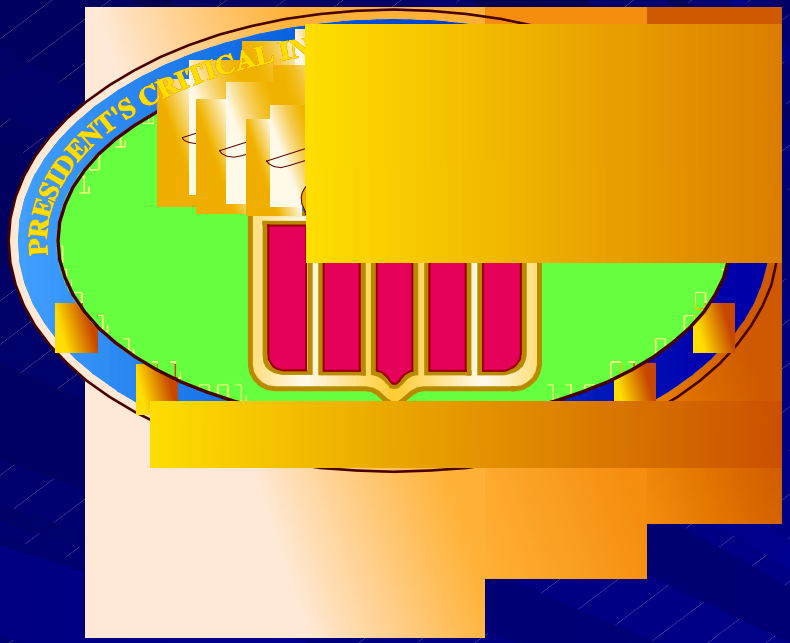
- ISTPA - International Security, Trust, and Privacy Alliance www.istpa.org
- An open, policy-configurable model of privacy services and capabilities
- ISTPA will work with Carnegie Mellon to enhance Framework and develop a Digital Privacy Handbook

The Privacy Framework

- Audit
- Certification of credentials
- Control - only permissible access to data
- Enforcement - redress when violation
- Interaction - manages data/preferences
- Negotiation
- Validation - checks accuracy of pers. info.
- Access - subject can correct/update info.
- Usage - process monitor

Strategy - Draft

- Govt. commitment to enforcement
- Consult with privacy advocates
- Expand GISRA audits to include privacy
- Encourage industry protect privacy
- Federal government lead by example
- Educate end-users about privacy; encourage informed choices



Andy Purdy, 202-456-2821

andy_purdy@nsc.eop.gov