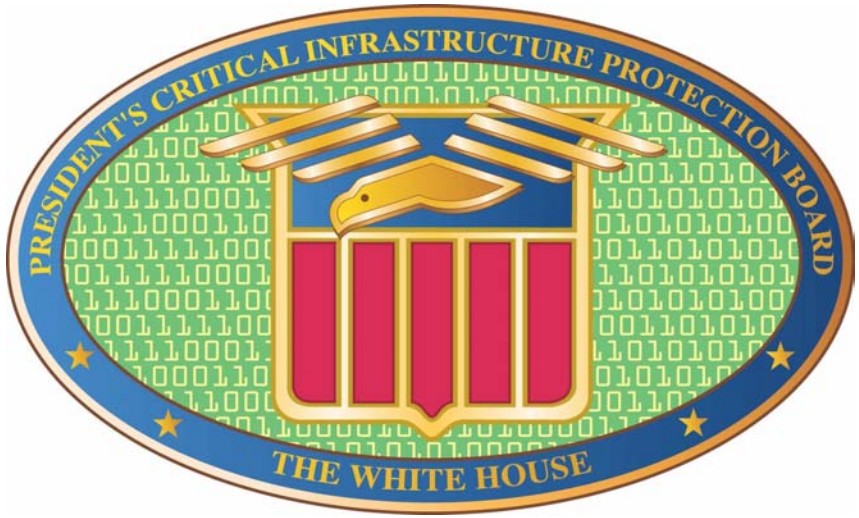
The National Strategy to Secure Cyberspace: Privacy, Security, and Healthcare



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

August 23, 2002

OVERVIEW

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

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.

Lessons Learned

- 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.

Lessons Learned

- 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

A New Paradigm

- Stop focusing on specific threats
- Focus on vulnerabilities

Executive Orders of the President – Oct 2001

Office of Homeland Security EO-13228 **8 Oct**

…to develop and coordinate a comprehensive national strategy to secure the United States from terrorist threats or attacks.

Critical Infrastructure Protection Board EO-13231 **16 Oct**

…to the protection of information systems and networks supporting critical infrastructures.

Homeland Security

- Physical security
  - Strategy released
- Cybersecurity
  - President's Critical Infrastructure Protection Board
  - Strategy to be released September 18, 2002

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

Who runs the Board?

The Chairman and Vice-Chair are appointed by the President.

They report to the President thru Governor Ridge or National Security Advisor Dr. Condi Rice.

The Chair also serves as Cyberspace Security Advisor to the President.

THE PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

Who is on the Board?

Senior Officials of Executive Branch departments

(typically Deputy or Under Secretary)

And the White House offices of the Vice President, Chief of Staff, National Security Advisor, Homeland Security Director, Management & Budget Director, Science Advisor

THE PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

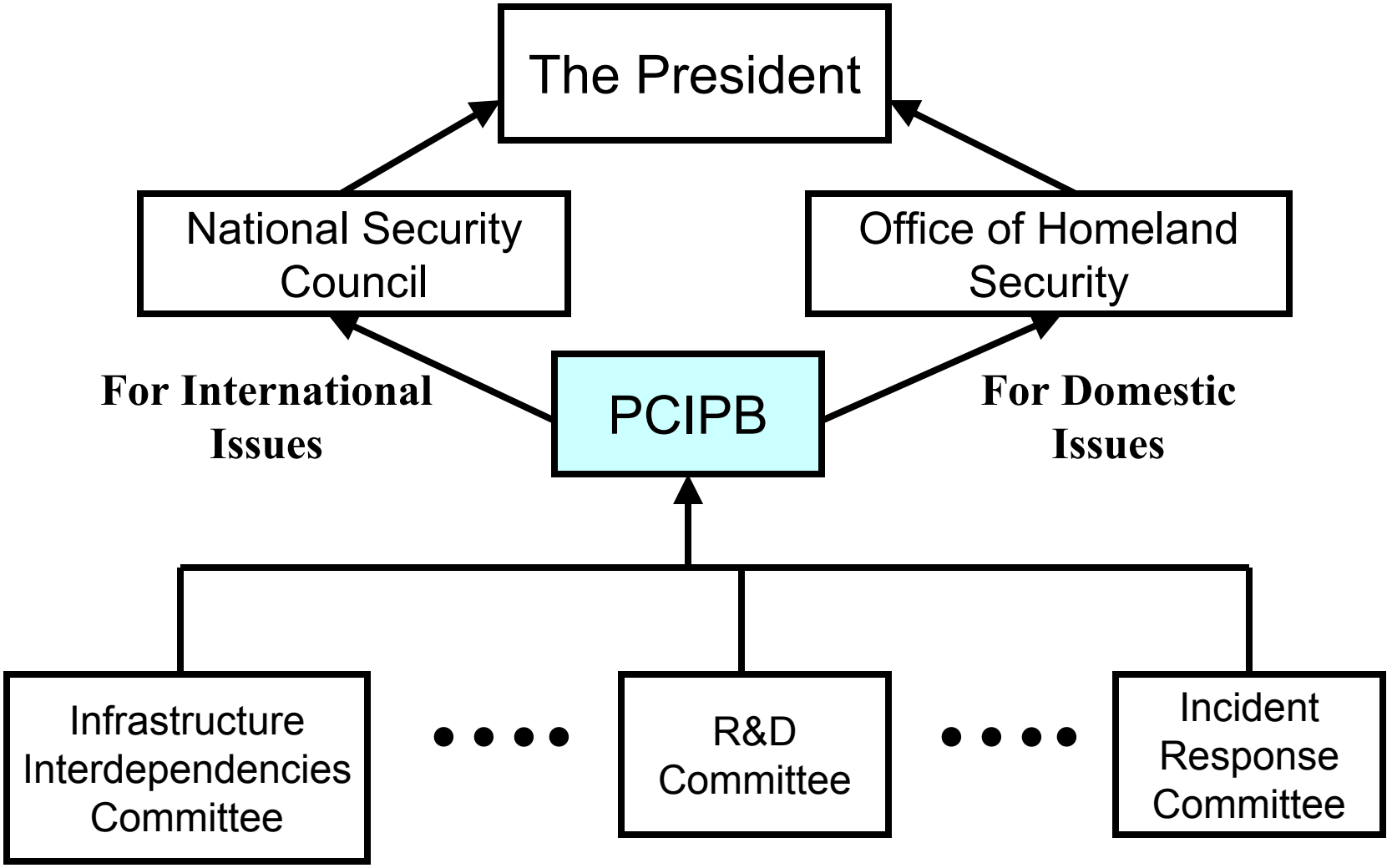
How does this relate to Homeland Security?

The Board, its Committees, and its Staff are the single Executive Branch system for Cybersecurity. They perform that function for both Homeland Security and National Security.

The Board can refer issues to the Cabinet level Homeland Security Council or to the NSC Cabinet level.

The Board Staff coordinates closely with both the Homeland and NSC staffs.

Relationships



Is the Board a new Bureaucracy?

No, the Board coordinates existing agencies.

The Board's Staff is ~20 people, many dual-hatted with OMB and NSC staffs.

The Board has a policy, not operational role, but its 10 committees do have operational responsibility.

Each committee has a Lead Agency as its Chair.

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

How does this relate to Homeland Security?

VERY CLOSELY!

The Board, its Committees, and its Staff are the single Executive Branch system for Cybersecurity, performing this function for both Homeland Security and National Security.

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 governments**
- **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 to create a National Strategy to Secure Cyberspace

--release set for September 18, 2002

--prepared with the private sector critical infrastructure companies

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

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

THE PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

Is the Board limited by its lack of budget authority?

The President authorized the Board to make recommendation on the Federal IT security budget.

The Board Staff works closely with OMB throughout the year.

The FY03 Budget submitted by President Bush in February, 2002 included a record 64% increase in funding for IT security programs to protect Federal departments' computer systems.

(IT security is now $4b out of overall Federal IT spending of $52b.)

National Strategy to Secure Cyberspace

- Introduction
- Case for Action
- Policy and Principles
- Highlights
- Level 1: Home Users and Small Business
- Level 2: Large Enterprises
- Level 3: Sectors
  - Federal
  - State and Local
  - Higher Education
  - Private Industry
- Level 4: National Priorities
- Level 5: Global

PDD-63 Critical Infrastructure Sectors

SECTOR	LEAD FEDERAL AGENCY
Information and Communications	Department of Commerce
Banking and Finance	Department of the Treasury
Water Supply	Environmental Protection Agency
Aviation, Highways, Mass Transit, Pipelines, Rail, Waterborne Commerce	Department of Transportation
Emergency Law Enforcement Services	Department of Justice/Federal Bureau of Investigation

PDD-63 Critical Infrastructure Sectors

SECTOR	LEAD FEDERAL AGENCY
Emergency Fire Service, Continuity of Government Services	Federal Emergency Management Agency
Public Health Services	Department of Health and Human Services
Electric and Power, Oil and Gas Production and Storage	Department of Energy
Federal Government	General Services Administration

Level 3 - Private Sector

EXAMPLE

Sectors Prepare Strategies

- Electricity (NERC)
- Oil & Gas (NPC)
- Water (AMWA)
- Rail (AAR)
- Banking & Finance (Morgan Stanley, BITS, et al.)
- Information & Communications (ITAA, TIA, CTIA, USTA)

Lead Agencies Summarize

Dept. of Energy

Dept. of Energy

EPA

Dept. of Transportation

Dept. of Treasury

Dept of Commerce (NTIA) /Dept of Defense (NCS)

Appendices

Strategy Text

National Cyber Priorities

Securing shared systems	Securing the mechanisms of the Internet Digital Control Systems Research Highly secure and trustworthy computing Securing emerging systems Vulnerability remediation Physical security
Creating a reinforcing economic and social fabric	Awareness Training and Education Certification Information sharing Crime Regulation and market forces Privacy
Developing national plans and policy	Continuity of operations, reconstitution and recovery National security Interdependency and Physical security Warning and analysis

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 - Development of secure operating systems - Expand the Institute for Information Infrastructure Protection's R&D agenda gap analysis program - Develop security enhancements for adhoc networks and grid computing
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
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

National Strategy for Homeland Security

Scope is directed by Executive Order 13228:

The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.

National Strategy for Homeland Security

- Executive Summary
- Introduction
- Threat and Vulnerability
- Organizing for a Secure Homeland
- Critical Mission Areas
- Foundations
- Costs of Homeland Security
- Conclusion: Priorities for the Future

www.whitehouse.gov/homeland/book/index.html

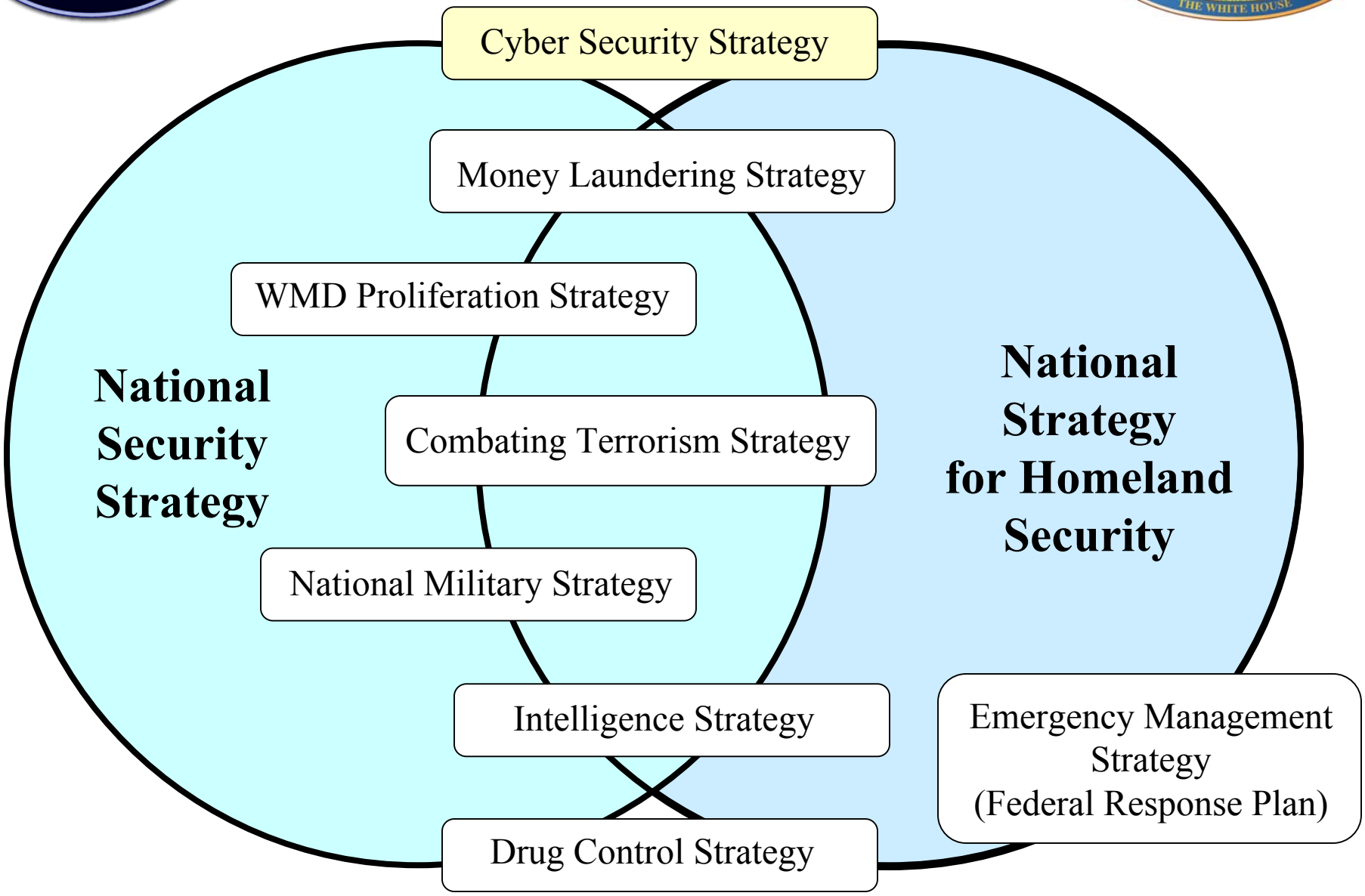
Critical Mission Areas for Homeland Security

Intelligence and Warning	- Enhance FBI analytic capabilities - Build new capabilities through information analysis and infrastructure protection division within DHS - Implement Homeland Security Advisory System - Utilize dual-use analysis to prevent attacks - Employ "red team" techniques
Border and Transportation Security	- Accountability in border and transportation - Create "smart borders" - Increase security of international shipping containers - Recapitalize the U.S. Coast Guard - Reform immigration services
Domestic Counterterrorism	- Improve intergovernmental law enforcement - Facilitate apprehension of potential terrorists - Continue ongoing investigations and prosecutions - Complete FBI restructuring to emphasize prevention of terrorist attacks - Target and attack terrorist financing - Track foreign terrorists and bring them to justice

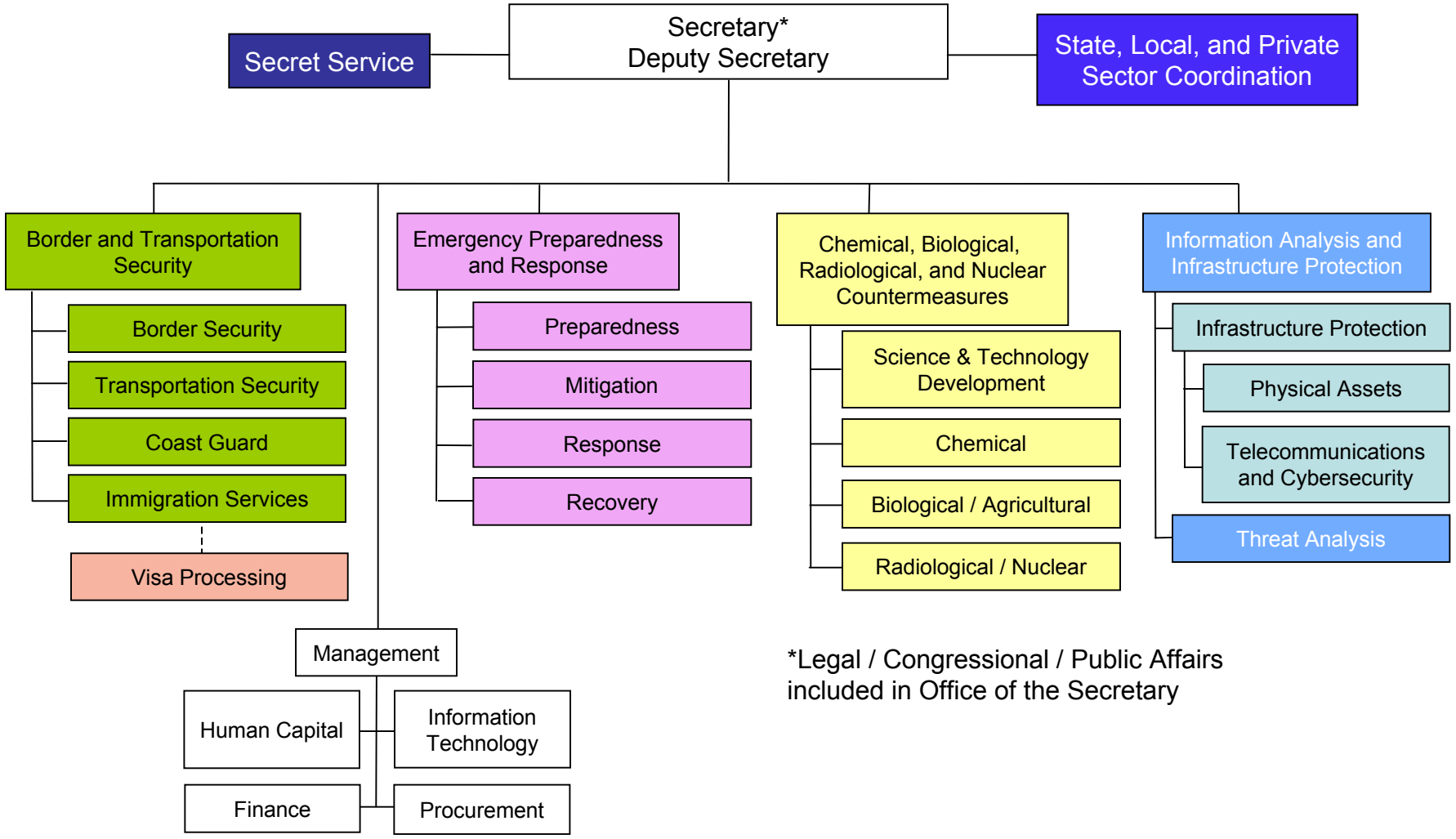
Critical Mission Areas for Homeland Security

Defending against Catastrophic Threats	- Prevent terrorist us of nuclear weapons through better sensors and procedures - Improve chemical sensors and decontamination techniques -Develop broad spectrum vaccines, antimicrobials, and antidotes - Harness scientific knowledge and tools to counter terrorism - Implement the Select Agent Program
Emergency Preparedness and Response	- Integrate separate federal response plans into one - Create national incident management system - Improve tactical counterterrorist capabilities - Enable seamless communication among all responders - Prepare health care providers for catastrophic terrorism - Augment America's pharmaceutical and vaccine stockpiles - Prepare for chem, bio, rad, and nuclear decontamination - Plan for military support to civil authorities - Build the Citizen Corps - Implement First Responder Initiative of FY03 budget - Build national training and evaluation system - Enhance victim support system

National Strategies



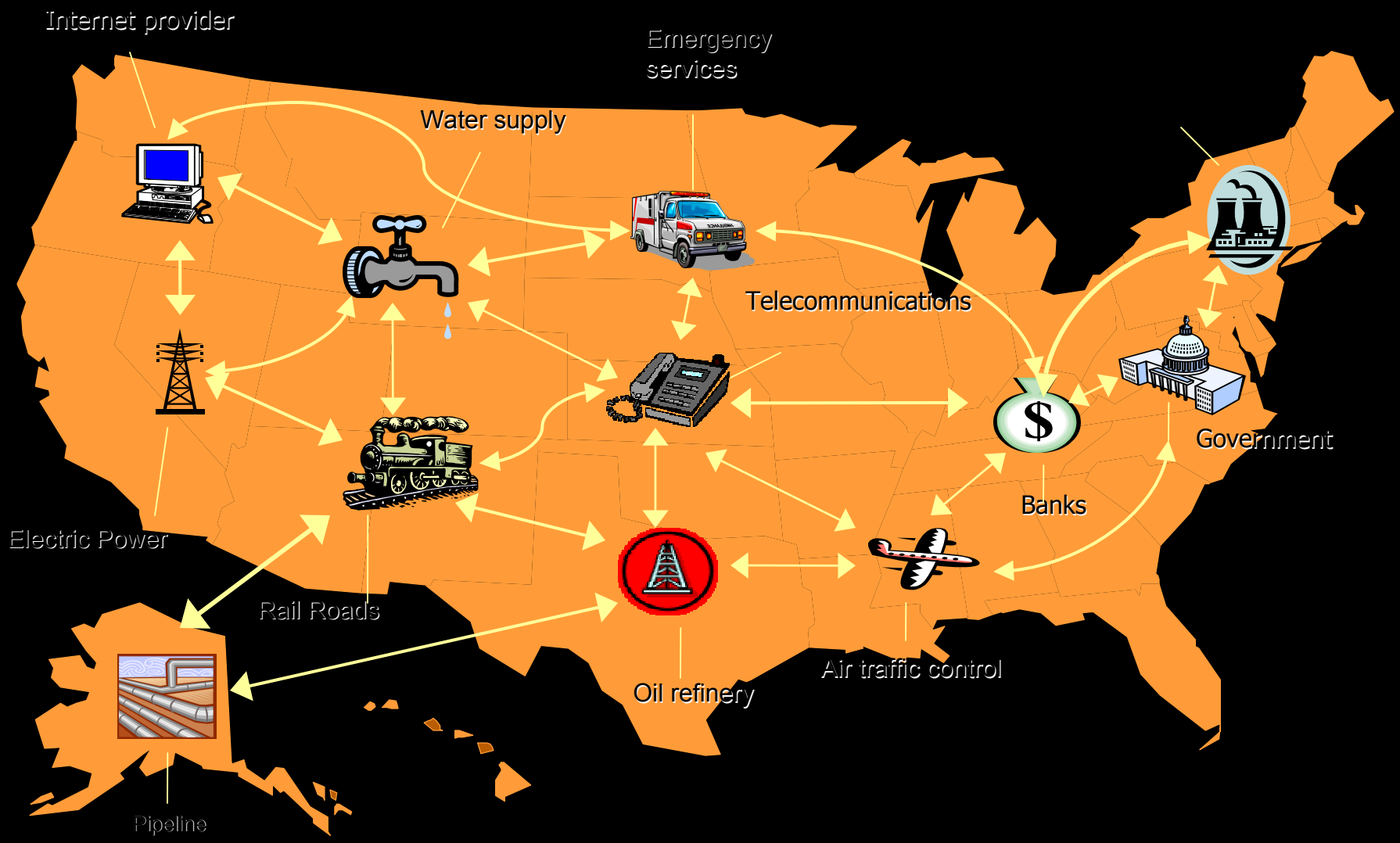
Department of Homeland Security



*Legal / Congressional / Public Affairs included in Office of the Secretary

www.whitehouse.gov/deptofhomeland/

Critical Infrastructure



Courtesy Sen. Robert Bennett (R-Utah)

September 11th 2001

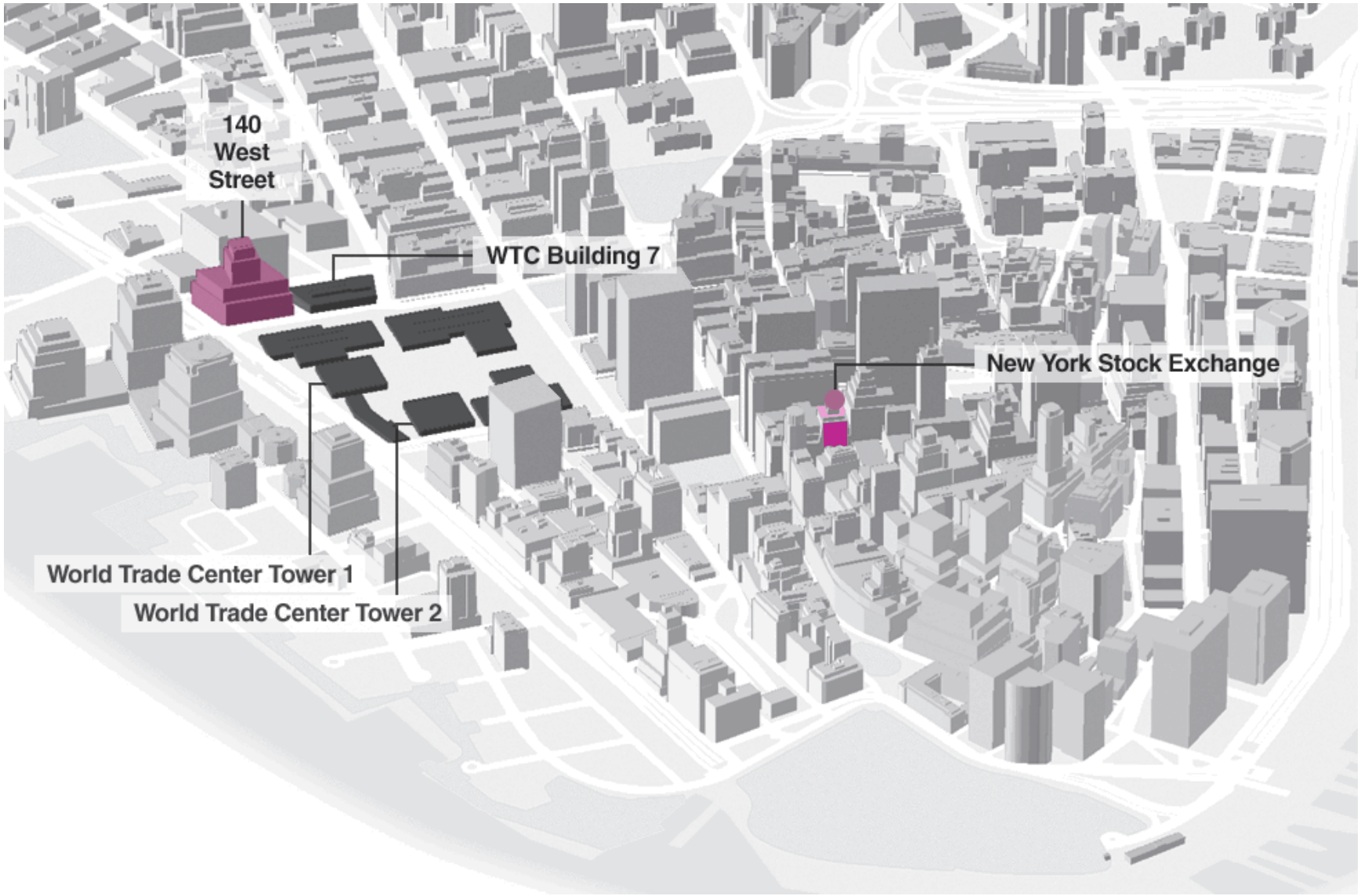
White House photo by David Bohrer

Secure in the Presidential Emergency Operations Center, Vice President Dick Cheney confers with President Bush via telephone and senior staff, including Karen Hughes and Dr.Condoleezza Rice

Impact on Communication Systems in New York City

- New York and American Stock Exchanges
- Verizon telephone building
- Plain old telephone system (POTS)
- Cell phone systems
- Wired and wireless Internet

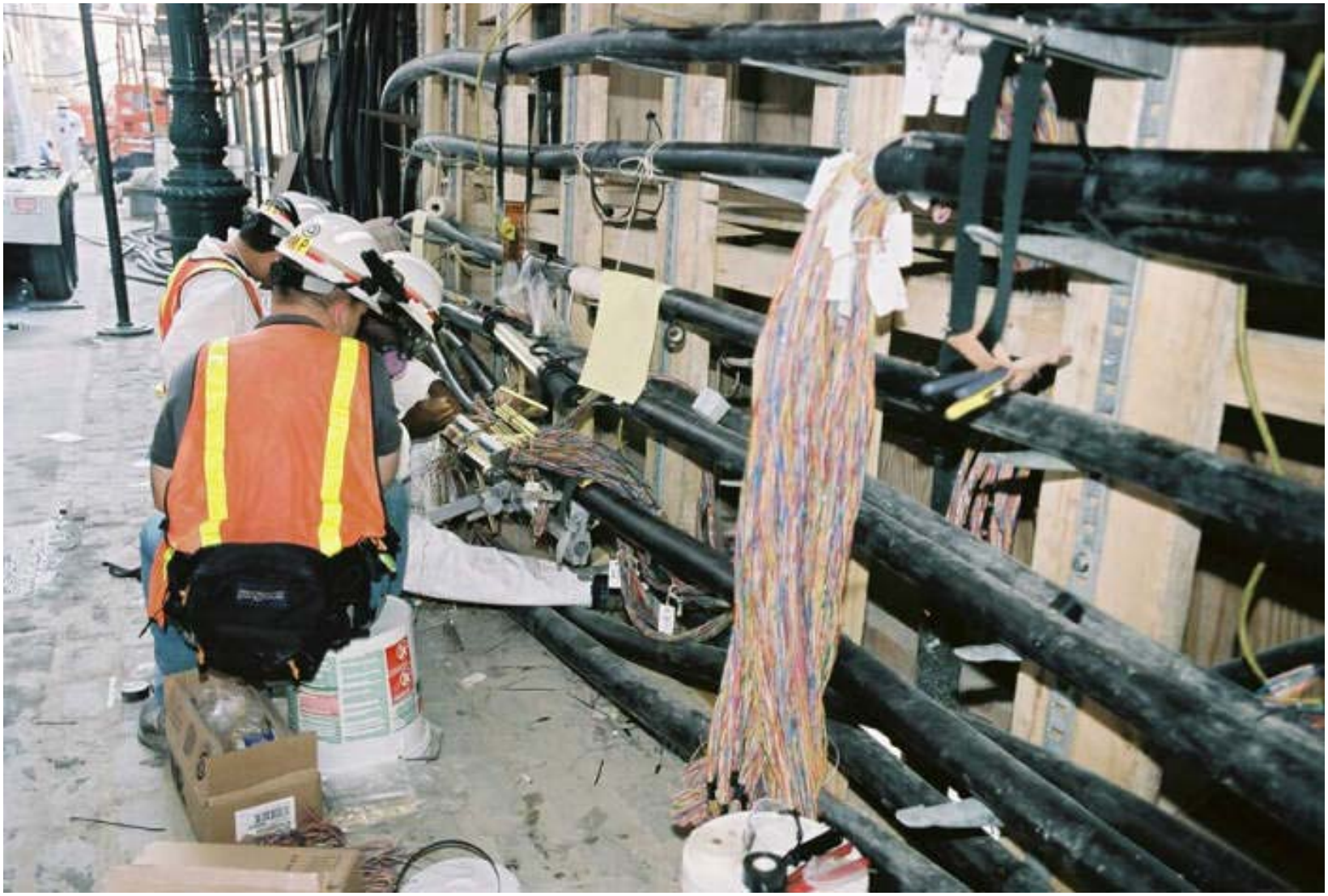
Lower Manhattan



Verizon Building
140 West Street

- 300,000 voice lines (200k for homes/small businesses)
- 3.5 million data circuits, 2 million that “pass through”
- 1,737 employees (all evacuated)
- Directly across the street from ground zero and next door to 7 World Trade Center
- Holes ripped in walls, girders pierced like arrows
- Water from broken mains and fire hoses flooded basement vaults, shorting cables that had not been cut by the falling steel
- Ducts outside were covered by 30 foot high debris, denying Verizon access for several days

Cable Repairs



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
versus
Security

- Access to more information can increase security.
- Surveillance and accessing personal information can reduce privacy.

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.

Privacy and Security

- There will be no privacy without security.
- Building in security is easiest during times of system overhaul and/or advances in technology.
- Expanded use of information technology makes it essential that security considerations be included at each stage: *inception*, *implementation*, and *in practice*.

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

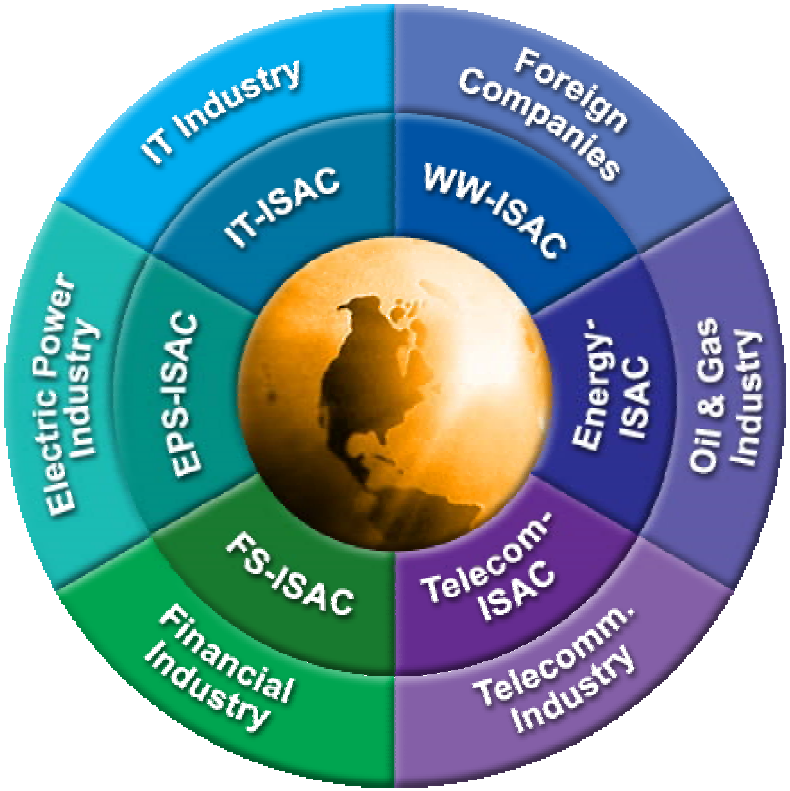
- Audit
- Certification of credentials
- Control - only permissible access to data
- Enforcement - redress when violation
- Interaction - manages data/preferences
- Negotiation
- Validation - checks accuracy of pers. info.
- Access - subject can correct/update info.
- Usage - process monitor

Health Care
A Critical Infrastructure

- Is health care a sector in need of an Information Sharing and Analysis Center (ISAC)?

Information Sharing and Analysis Centers (ISAC)

- Vital part of critical infrastructure protection
- Gather, analyze, and disseminate information on security threats, vulnerabilities, incidents, countermeasures, and best practices
- Early and trusted advance notification of member threats and attacks
- Organized by industry: cross-sector awareness, outreach, response, and recovery



Looking at the Health Care Sector

- What are the subsectors:
  - state/county health depts.,
  - hospitals,
  - insurers,
  - HMOs,
  - medical professionals,
  - medical device companies,
  - pharmaceuticals - others?

Health Care Sector

- “Focus” meeting convened by White House earlier this month with reps of subsectors to discuss ISAC issues.
- Govt.: HHS, CIAO, CDC, state/county depts.
- Private sector reps.
- Followup meeting to be hosted by American Hospital Assoc. .

Health Care Sector

- Q: What are interdependencies?
  - Between subsectors?
  - Between health care and other sectors?
- A: Initial perception - not very.

Health Care Sector - The Present

- Are interdependencies a concern now?
- How independent is the sector? What about:
  - Electric power?
  - Communications?
  - Water?
  - Transportation?

Health Care Sector - The Future

- "Focus" meeting: information technology is burgeoning.
- What are the trends:
  - Record access
  - Online ordering
  - Diagnosis/testing
  - Monitoring
  - Insurance coverage
  - Identification
  - Payment

Health Care Sector - The Future

- Increasing technology means:
  - Increasing interdependency
  - Increasing vulnerability
- Is security playing the appropriate role in ensuring the safety and reliability of the sector?

Are you ready?

- How many times a day do Americans seek medical care or prescriptions? A week?
- What if systems are shut down for several days...or a week…or a month?
- What would happen to health care delivery in this country?

Is anyone ready?

- For simultaneous cyber and physical attacks?
- (so-called “swarming” attacks)

Common Themes

- How to be prepared?
  - Prevention
  - Systems to minimize damage
  - Redundancy (backup)
  - Remediation

Common Themes

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

Supplemental Information

Protecting America's Critical Infrastructures:

1998 Presidential Decision Directive 63

Established four new organizations:

- National Infrastructure Protection Center (NIPC)
- Information Sharing and Analysis Centers (ISACs)
- National Infrastructure Assurance Council (NIAC)
- Critical Infrastructure Assurance Office (CIAO)

and several "sector liaisons" such as:

- Dept of Energy – Electric Power Sector
- Dept of Treasury – Banking and Finance Sector
- Dept of Commerce – Telecommunications Sector

National Infrastructure Protection Center

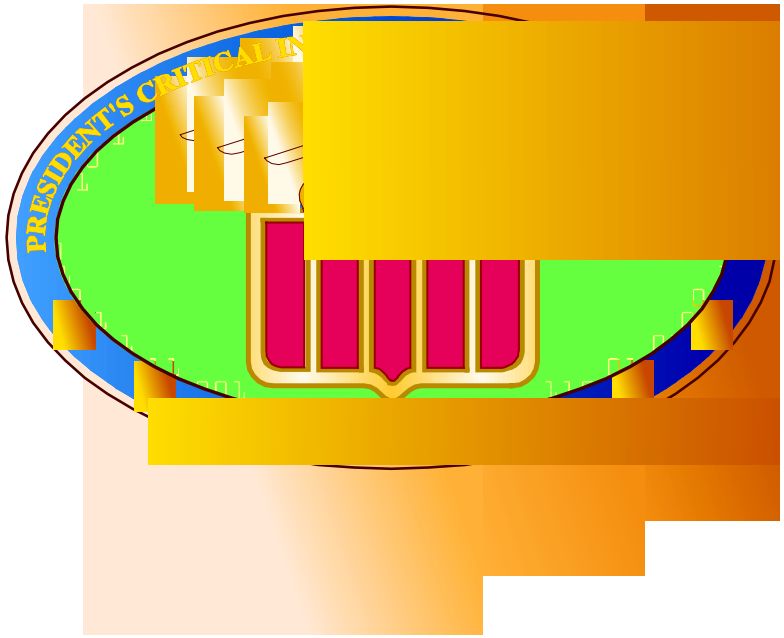
- Located in the FBI's headquarters in Washington, DC
- Representatives from US government agencies, state and local governments, and the private sector
- Established in February 1998
- Mission is to serve as the US government's focal point for threat assessment, warning, investigation, and response for threats or attacks against US critical infrastructures

National Infrastructure Protection Center

www.nipc.gov

Critical Infrastructure Assurance Office

- Housed within the U.S. Commerce Department's Bureau of Export Administration
- Established in 1998
- Coordinates the Federal Government's initiatives on critical infrastructure assurance
- Major initiatives include
  - Coordinate and implement the national strategy
  - Assess the U.S. Government's own risk exposure and dependencies
  - Raise awareness and educate public understanding
  - Coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors



Andy Purdy, 202-456-2821

apurdy@nsc.eop.gov