HOMELAND SECURITY

Collaboration Innovation and Standardization

2003 ANSI Annual Conference

ANSI

American National Standards Institute

Critical Infrastructure Protection: Two of Many Standards Needs

presented by

Ken Watson

President and Chairman

Partnership for Critical Infrastructure Security

ANSI

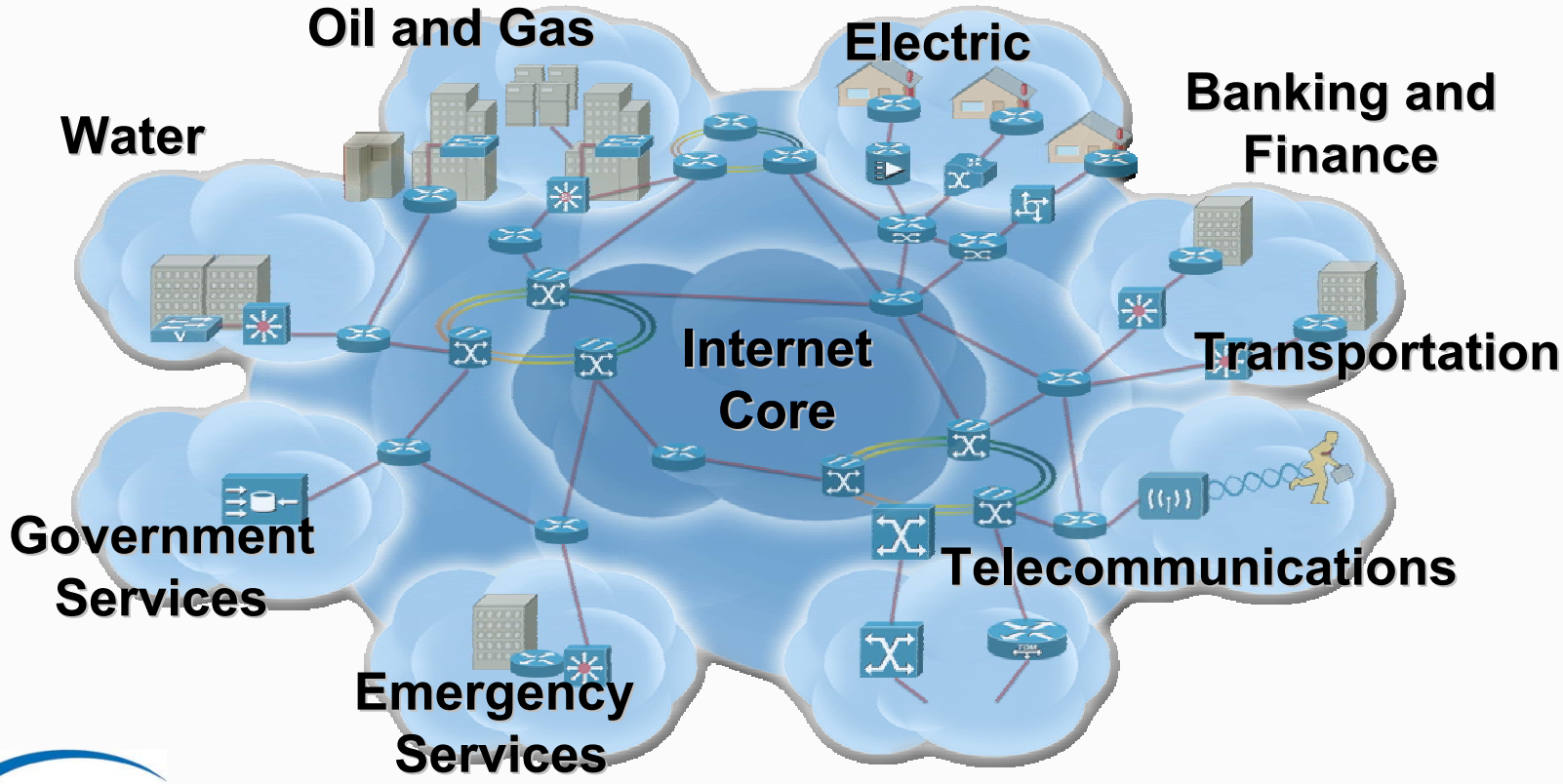
American National Standards Institute

Critical Infrastructure Protection: Two of Many Needs

- Agenda
  - Critical Infrastructure Protection background
  - Two Key Standards Needs
    - Information Sharing
    - Manufacturing and Control Systems
  - Current Control System Standards Activities
  - Information Sharing Recommendations

The World is a Network of Networks…

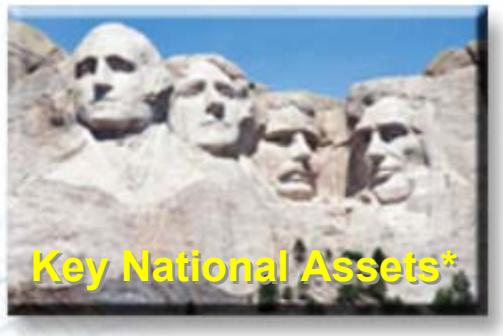
Any Geographical Area, Any Network, Any Functional Area Is a Place of Vulnerability



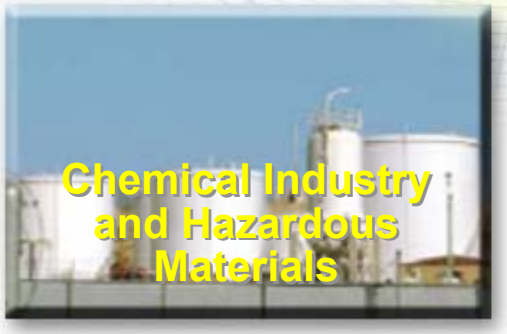
Critical Infrastructures

PDD-63 Critical Infrastructures

Critical Infrastructures



Added Critical Infrastructures



National Security Interest

Infrastructures…

- **Are critical to safety, security, our way of life**
- **Depend on commercial networks**
- **Are interdependent**
- **Are largely owned and operated by private companies**
- **Cannot entirely depend on the Federal government for defense against cyber attacks**

Government Needs Industry in a True Public-Private Partnership

The Business Case

- **Businesses dependent for their survival on the Internet**
- **Vulnerabilities threaten economic survivability and competitiveness**
- **Interdependency**
  - **Supply chain**
  - **Partners**
  - **Customers**
  - **Infrastructure industries**
- **Companies are on the front lines of defense**

Industry Needs Government in a True Public-Private Partnership

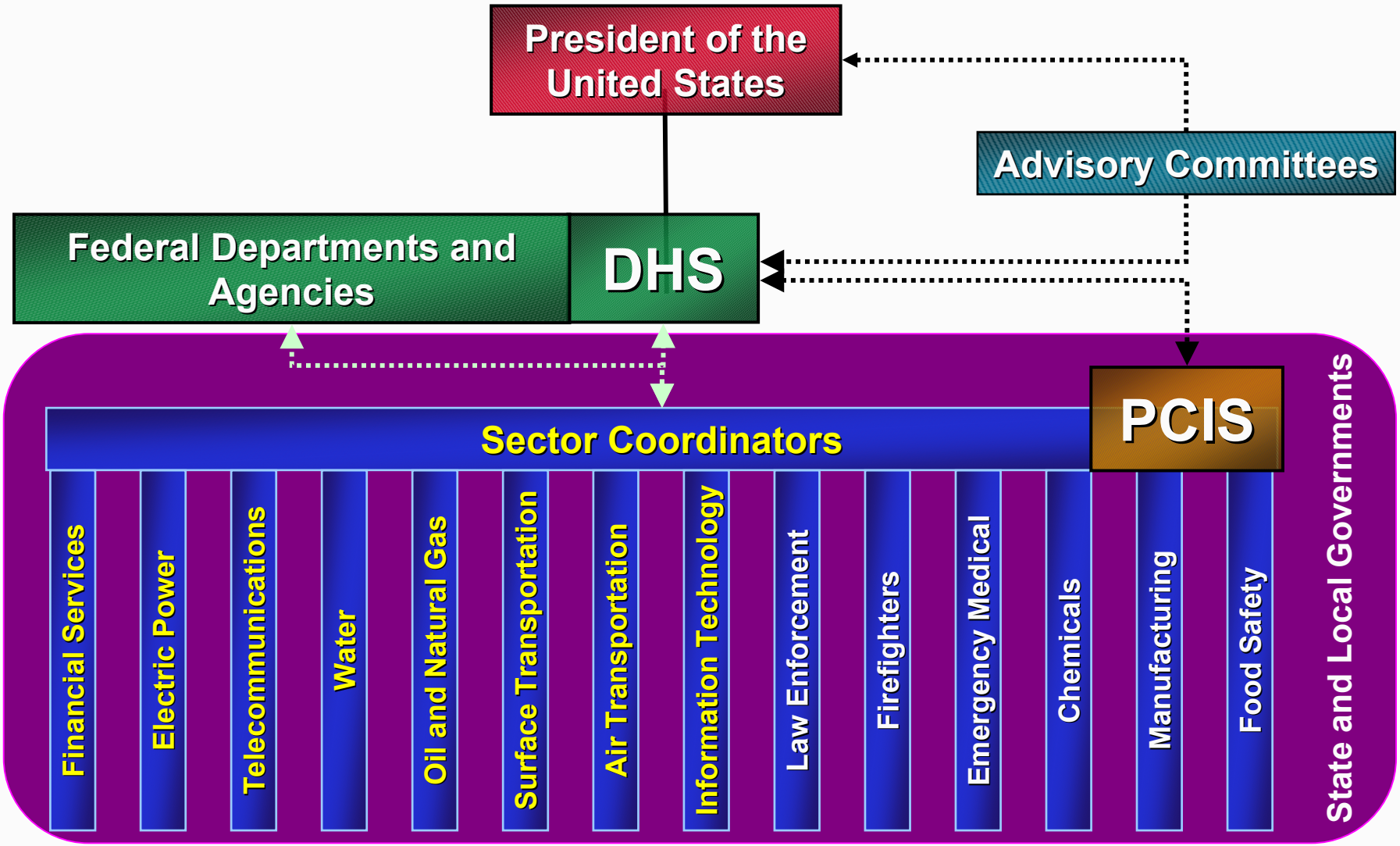
Cross-sector Collaboration

Partnership for Critical Infrastructure Security (PCIS)

http://www.pcis.org

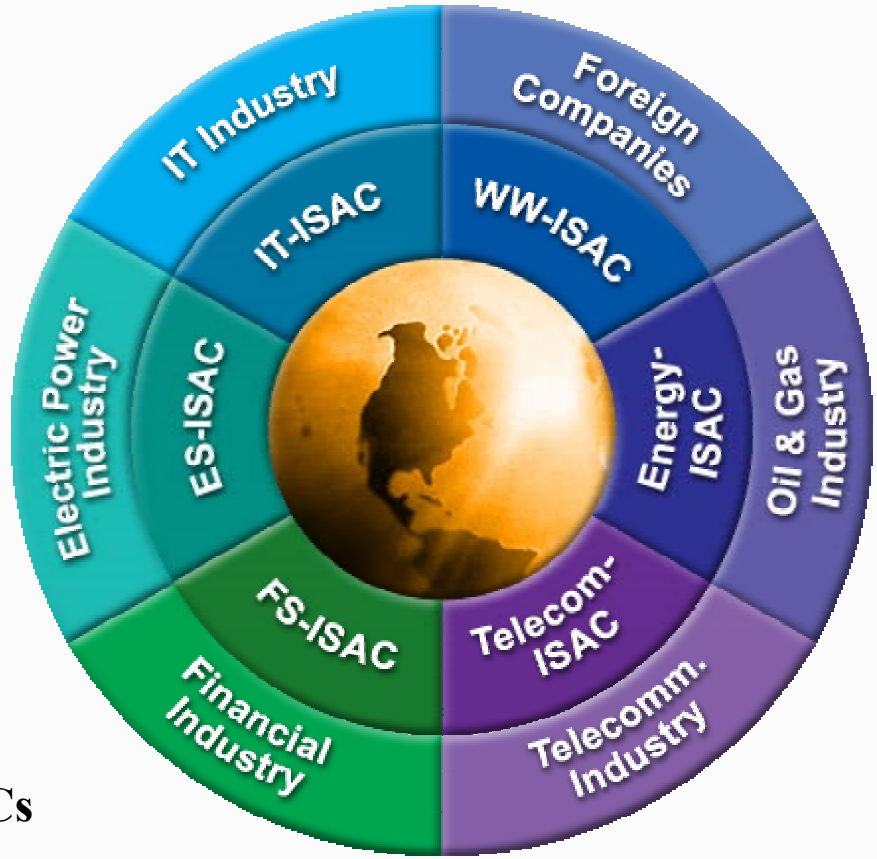
- Participation by leaders from government, industry & academia
- Coordinates cross-sector initiatives and compliments public-private efforts
- Board of Directors majority *always* critical infrastructure "sector coordinators"

US Public-Private Relationships for CIP



Information Sharing and Analysis Centers (ISACs)

- Vital part of Critical Infrastructure Protection (CIP)
- 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
- ISAC Council: Leadership of ten ISACs



Need for Information Sharing Standards

- **10 ISACs + DHS: Unique alert levels, message formats, requirements**
- **Vulnerability disclosure *complex* issue**
  - **National Infrastructure Advisory Council (NIAC) developing guidelines**
- **PCIS taxonomy effort—6000 terms**
  - **http://www.pcis.org/library.cfm?urlSection=WG (first two listings)**
- **ISAC Council working on cross-sector and public-private information sharing mechanisms**
- **Must consider physical and cyber aspects**

Need for Common IT/Control System Risk Analysis Standards

- Control system networks are becoming more like IT networks
- Plant/control system engineers understand safety risk assessments; IT security engineers understand information security risk assessments
- Cyber incident data much more scarce than accident data—deliberate cyber attacks hard to quantify
- Therefore, need common physical and cyber analysis tools
  - Methodologies similar for both aspects
  - Interdependencies

Current Control System Cybersecurity Standards Activity

- **American Gas Association AGA-12-1: draft standard currently in development for protecting legacy Supervisory Control And Data Aquisition (SCADA) communications links**
  - **See http://www.gtiservices.org/security/**
- **Instrumentation Systems and Automation Society (ISA) SP-99: cross-sector cybersecurity initiative**
  - **Aimed at attempts to do the best with *existing* technology and practices**
  - **Two reports:**
    - **TR-1 (Technology)**
    - **TR-2 (Application and Practice)—out for ballot 16 Sep 2003**
  - **See http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821**
- **NIST Process Control Systems Security Requirements Forum (PCSRF): draft "Security Capabilities Profile" document to serve as the basis for writing protection profiles for different control systems components**
  - **Aimed at *next generation* of control system networks and products**
  - **See http://www.isd.mel.nist.gov/projects/processcontrol/**

Information Sharing Recommendations

- **Leverage ongoing work**
  - **NIAC Vulnerability Disclosure guidelines**
  - **ISAC Council procedures**
  - **PCIS "dictionary"**
- **Work toward standard:**
  - **Message formats**
  - **Terms**
  - **Alert levels (where applicable)**