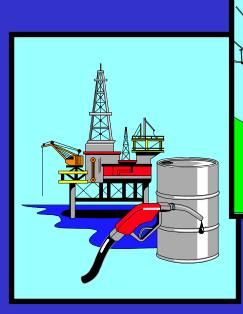
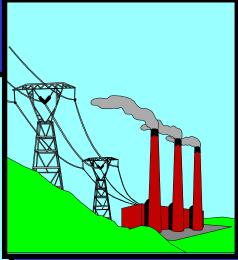


Energy Sector

The Lifeblood of the Critical Infrastructures

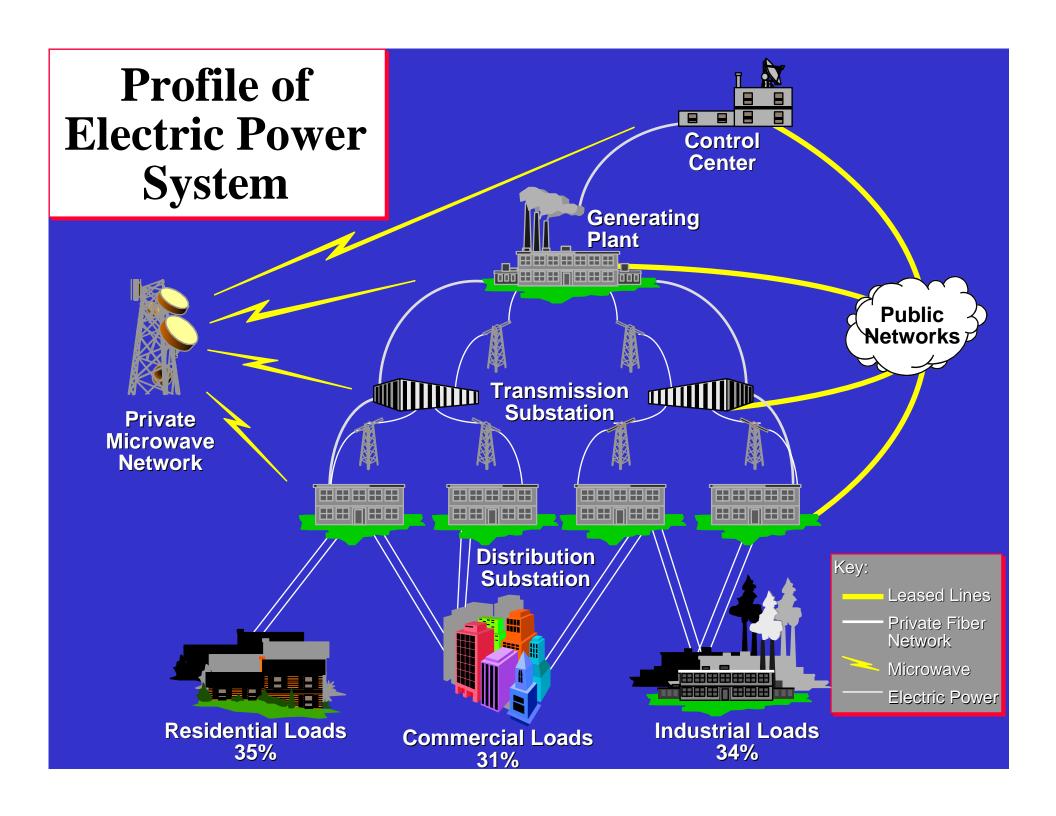




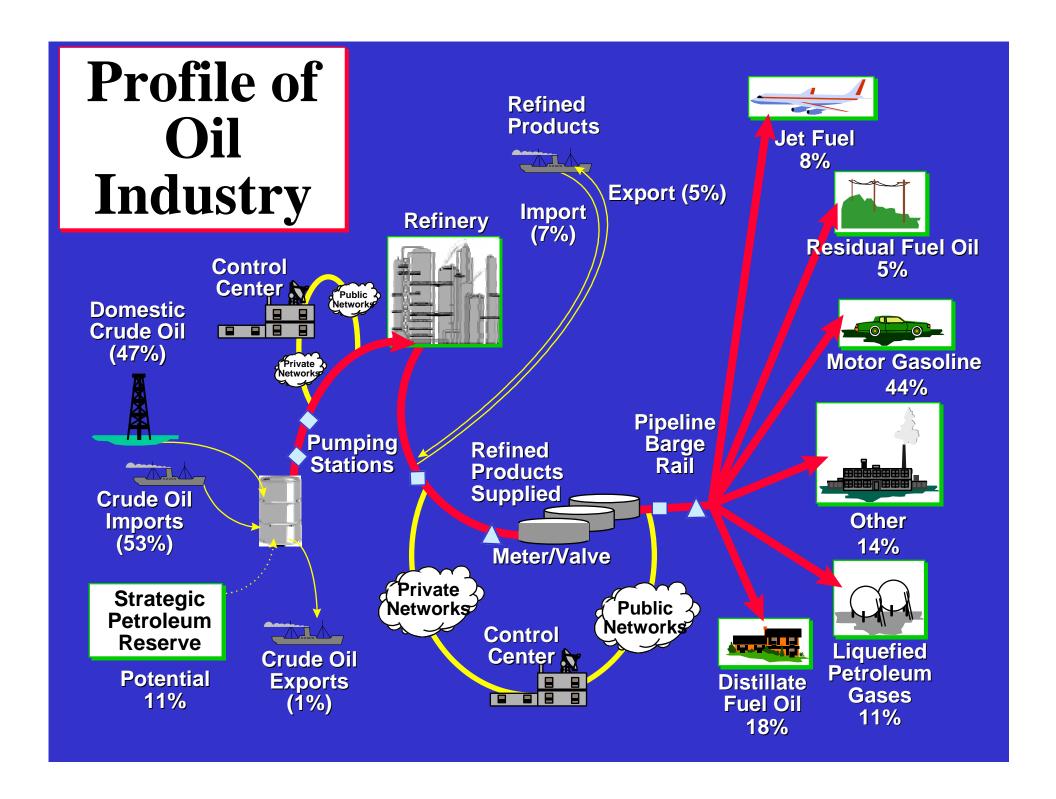
Electricity
Natural Gas
Oil

David JonesCommissioner

President's Commission On Critical Infrastructure Protection



Profile of Control **Natural Gas** Center Residential Interconnection 25% Industry **Points** Private **Networks Natural Gas** Public Canada Networks-**Processed** Commercial 12% 15% Receipt **Points** City Gate **Delivery** Compressor **Points** Industrial Meters/ Station 44% Valves **Pipelines Gross** Withdrawals **Electric From Gas Utility** & Oil Wells 16% **Natural Gas** Storage Facilities Processing & Production | Gathering Distribution Transmission: Storage





- Electric power and natural gas restructuring
 - Mergers, marketing, financial systems, consolidation of resources, downsizing, reduced reserves/capacity
 - Reliability concerns
- Significant increase in use of natural gas
- Oil
 - Lower profit margins
 - Downsizing
- Dependence on information



Energy Data Base Documents over 15,000 World-Wide Incidents (1,000 in U.S.) During Last 15 Years

- → June 1992 emergency alert alarm system software modified
- → July 1996 London infrastructure IRA attack interrupted



- Major expansion of information systems
- Commercial Off the Shelf (COTS) products
- Internet
- Supervisory control and data acquisition systems
- Availability of tools to exploit cyber vulnerabilities
- Availability of targeting/critical node information
- Physical vulnerabilities of critical assets

Integrated Utility Network

Power Plant Network

Control Center Network

Real-Time SCADA Network

Data Exchange Wide-Area Network

> Transmission Network

External Networks

Company Wide-Area Network

Corporate Network

Distribution Automation /

Customer Interface Network

Energy Sector

President's Commission on Critical Infrastructure Protection



- Information sharing
- Cyber intrusion database
- Training & awareness
- Information assurance tools
- Physical & cyber security best practices/standards



Preliminary Recommendations

- Enhance information sharing
- Process to protect sensitive private sector information shared with government
- Industry & government develop "best practices"
- Testbed/pilot project to demonstrate infrastructure assurance program
- Double research and development efforts



Preliminary Recommendations (cont'd)

- Industry recommendations to support:
 - Establish national standards for "one-call" program
 - Review/revise existing regulations on excessive reporting of sensitive information
 - Allow military/national guard use in time of war or credible terrorist threat
 - Form a joint center (government/industry) for sharing threat and vulnerability information
 - Joint effort industry and government to analyze cyber threats and develop countermeasures