President's Commission on
Critical Infrastructure Protection

Information & Communications Sector

The Nation's Central Nervous System

Nancy J. Wong
Commissioner

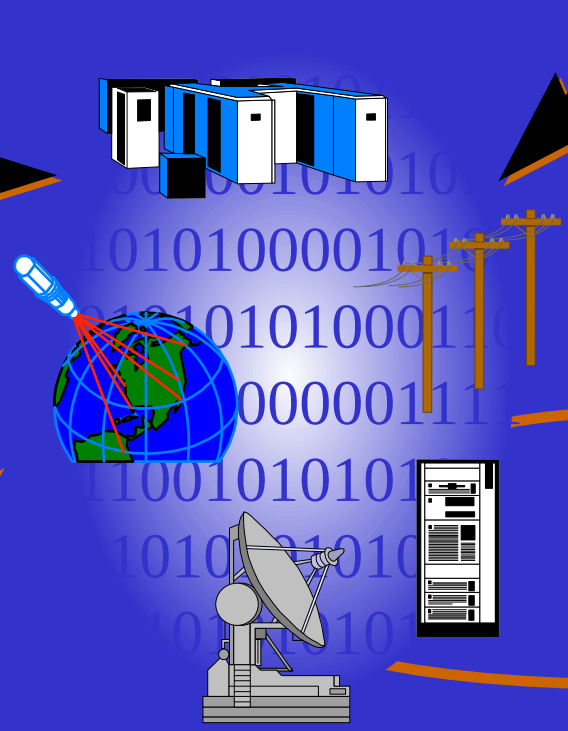
- **The Information Age:** ***Made In America***
- **Vulnerabilities & Threats**
- **Bottom Line Risk**
- **Preliminary Recommendations**

Infrastructure Service Delivery

Suppliers

- Services
- Hardware
- Software

Regulators and Legislators



Employees

Customers

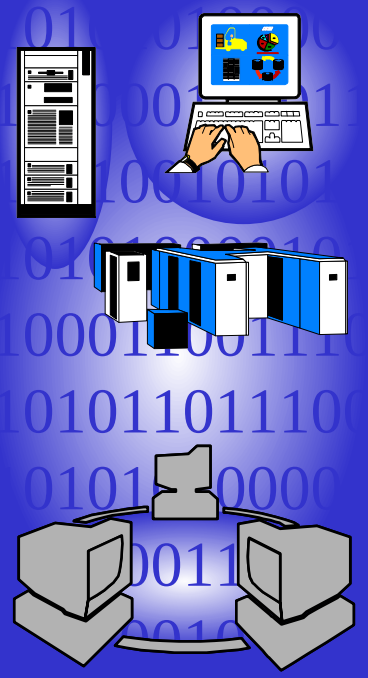
Owners/Operators

Information Technology Industry Characteristics

- $730 Billion/Year
- Globalized
- High turn-over, fast-moving innovation
- Telecommunications industry undergoing major restructuring and deregulation
- Many new market entrants in the near future

U.S. Dependence on Information Technology

- The U.S. uses:
  - 42% of the world's computing power.
  - 60% of the world's Internet assets.
  - 200 million connect hours/day.
- The U.S. has reshaped business and governmental processes around information and communications:
  - 90% of large and 75% of small companies have LAN's.
  - $40 billion/year Federal spending on information technology.
- This sector is the major source of interdependency accross the infrastructures



Sources of Vulnerabilities

- Concentration & complexity
- Industry restructuring
  - New access services & access points
  - More remote control for operations and maintenance
  - Global proliferation & foreign ownership
  - Rush to new technologies
- Broader population of “insiders”
- Insufficient physical & cyber security planning and implementation
- Open source access to information: the Internet
- Low cost of exploitation

Primary Sources of Threats

Reliability

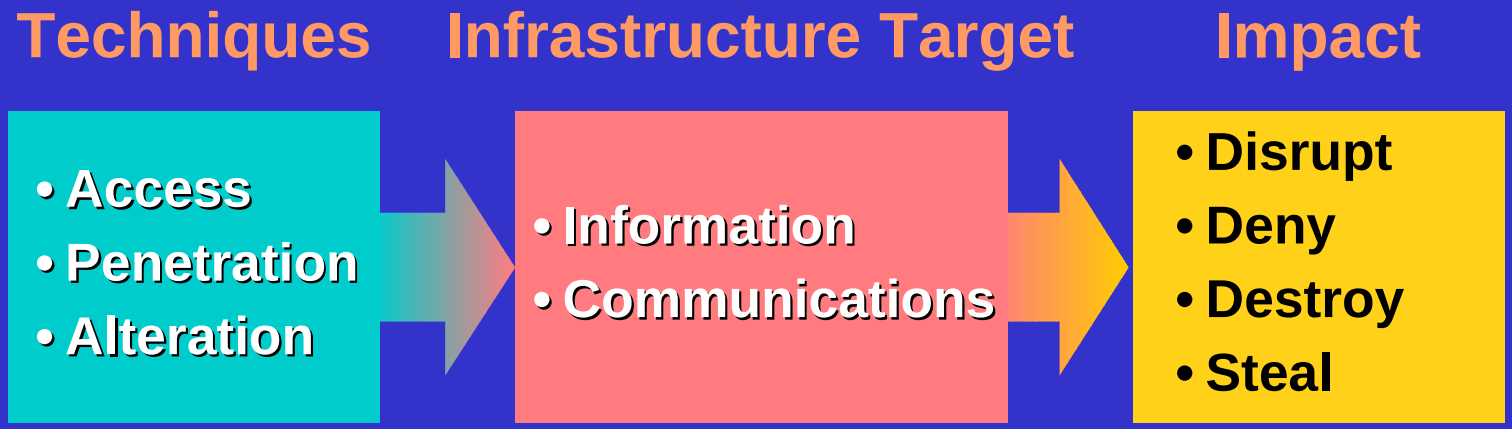
- Natural disasters
- System failures
- The “backhoe”

Security

- Deliberate physical and computer-based threats
- Two levels of risk

Computer-Based Security Threats

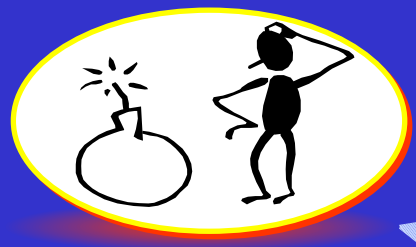
With *Intention* to Do Harm



- The tools, expertise, capability, and delivery mechanisms ***are available and accessible***
- The only trigger needed is a malicious intent, with a will and motivation to disrupt, deny, destroy, or steal

Bottom Line Risk

- It is improbable that, *tomorrow*, a determined group of hackers could bring down the nation's public telecommunications network
- However, pervasive dependence on this infrastructure yields noticeably greater magnitude of consequence in an adverse event
- Given "as is" level of protection investment in the face of growing pace of change, there is increasing likelihood that a disruption with national impact could occur *within the decade*
- Consequences can undermine public confidence as well as the bottom line



Preliminary Recommendations

Infrastructure Protection

- Take action to implement well-established basics of information assurance, pervasively throughout industry and government
- Manage the emerging telecommunications environment to sustain expected levels of performance
- Federal government leads by example as a national model for sound information assurance practices
- Develop a national technical capability to defend against computer-based attacks
- Enhance public/private partnership process(es)