



Critical Infrastructure Protection (CIP)

March 13, 2001

Critical Infrastructure Protection

❖ **Background**

- President's Commission on CIP
- Presidential Decision Directive 63

❖ **CIP Implementation Issues**

❖ **Information Sharing Models**

❖ **Questions**

Background

July 1996

President's Commission on Critical
Infrastructure Protection

May 1998

Presidential Decision Directive 63 -
Protecting America's Critical Infrastructure

President's Commission

❖ **Purpose**

- Assess Vulnerabilities
- Recommend National Policy and Implementation Strategy

❖ **Critical Infrastructures**

- Information and Communications
- Banking and Finance
- Water Supply
- Electric Power
- Oil and Natural Gas
- Transportation
- Government Services
- Emergency Services (Medical, Police and Fire)

President's Commission (con't)

❖ Findings

- Information sharing is the most immediate need
- Responsibility shared among industry and government
- Need integration of federal agencies
- Challenge: Adapting to a changing culture
- The federal government has important roles
- Existing legal framework is imperfect
- More research and development is needed

Background

July 1996

President's Commission on Critical
Infrastructure Protection

May 1998

Presidential Decision Directive 63 -
Protecting America's Critical Infrastructure

Presidential Decision Directive 63

❖ Purpose

- Call for a national effort to ensure the security of the nation's critical infrastructure
- Provide for a framework for working with the eight identified critical infrastructure sectors to develop plans and meet goals
- Implementation Timeframe:
 - 2000 - 'Initial' operating capability
 - 2003 - Full operating capability

Presidential Decision Directive 63

❖ **Implementation**

- Each sector lead by their governmental regulatory department or agency
- The lead agency appoints a 'sector coordinator'
- Each sector to provide a way to internally share information (e.g., ISAC)
 - Accumulate information
 - Disguise the identify of providers
 - Disseminate information to the sector owners and operators

Presidential Decision Directive 63

❖ **Implementation (con't)**

- Department of Commerce
 - Provide an awareness campaign and build the public/private partnership
 - Establish the Critical Infrastructure Assurance Office (CIAO)
- FBI
 - Establish the National Infrastructure Protection Center (NIPC)
 - Establish regional Infragard partnerships

CIP Implementation Issues

- ❖ **Each sector implementation differs**
- ❖ **New electronic and interconnected economy**
- ❖ **Legal and regulatory uncertainties**

CIP Implementation Issues (con't)

- ❖ **Vulnerabilities, Threats, and Consequences**
- ❖ **Information Sharing Needs and Concerns**
- ❖ **Risk Management and Vulnerability Mitigation**

CIP Implementation Issues (con't)

- ❖ **Research and Development Needs**

- ❖ **Y2K Model for Future Actions**

Information Sharing Requirements

- ❖ **Provide broadest range of threat, vulnerability, and incident data.**
- ❖ **Acquire data from the broadest range of global sources.**
- ❖ **Identify, analyze and disseminate threats and vulnerabilities globally and in real time.**
- ❖ **Analyze high volumes of data.**
- ❖ **Prioritize cyber incidents and provide timely alerts and solutions.**

Information Sharing Requirements

- ❖ **Provide members a choice to remain anonymous when reporting incidents.**
- ❖ **Provide single repository for access to threat, vulnerability, and incident identification and solutions.**

Information Sharing Models

❖ ISAC Implementation

- Financial Services (Citigroup)
- Oil and Natural Gas (NPC)
- Electric Power (NERC)
- Information Technology (ITAA)
- Telecommunications (NCC)

❖ Other Models

- Other industries (e.g., chemical, CDC)
- Infragard (NIPC)

CIP Questions

❖ **Questions?**

