

President's Commission on Critical Infrastructure Protection

Legal Recommendations Overview





Legal Landscape *Conclusion*

- ◆ “Infrastructure assurance” is really about instilling cultural change
 - Encouraging *businesses* to better manage emerging risk
 - Encouraging *government* to realign itself to address emerging threats and vulnerabilities
 - Encouraging *individuals* to practice better systems and information security at home and work

- ◆ We should also seek to promote cultural change within legal institutions
 - Federal, state, local, international
 - Raise awareness of infrastructure assurance concerns and objectives
 - Encourage closer examination of existing laws in light of those objectives

Legal Recommendations

New Challenges in Protecting Our Critical Infrastructures

Legal recommendations intended to address:

- ◆ emerging irrelevance of traditional geographic and jurisdictional boundaries
- ◆ growth in availability of wide range of tools and know-how for attacking critical infrastructures
- ◆ failure of the law to keep pace with emergence of networked environment and new threats to critical infrastructures
- ◆ organizational and institutional barriers to properly addressing infrastructure assurance-related issues



Legal Recommendations

OBJECTIVES:

- ★ *Improve Effectiveness of Government Assurance Efforts*
 - serve as model of sound practices
 - prevent, deter, and respond to attacks
 - aid in recovery from harmful events

- ★ *Enable Private Sector Protective Action*
 - take precautions against the insider threat

- ★ *Overcome Legal Impediments to Public-Private Partnership*
 - promote information sharing
 - promote public-private policy formulation



Legal Recommendations: *Increasing Effectiveness of Federal Assurance Efforts*

GOAL: Federal Government Take the Lead in
Adopting Appropriate Assurance Measures

- Adopt government “model performance” measures--actions that can be taken unilaterally by the federal government to improve its performance and influence the private sector
 - procurement practices
 - publication of infrastructure assurance data
 - certifications

- Clarify procedures to facilitate vulnerability assessments for government systems



Legal Recommendations: *Increasing Effectiveness of Federal Assurance Efforts*

GOAL:

**Federal Government Take the Lead in
Evaluating Effectiveness of Assurance
Measures**

- ⇒ Use strategic planning and performance measurement framework (GPRA) to highlight assurance responsibilities and initiatives
- ⇒ Amend ITMRA to require development of performance measures relating to system security



Legal Recommendations: *Increasing Effectiveness of Federal Assurance Efforts*

GOAL:

Improve Federal Government's Ability to Prevent, Deter and Respond to Attacks on Critical Infrastructures

- ➔ Enhance criminal law and procedure as applied to threats--*physical & cyber*--to critical infrastructures
 - Sentencing Guidelines
 - sentences should reflect “downstream” harm
 - sentences should reflect “informational” harm
 - Procedural Issues
 - Infrastructures as “instrumentalities” of interstate commerce
 - Reward programs for information leading to capture of terrorists
 - cross-jurisdictional trace and search court orders
 - continued support of international cooperative efforts
 - Study of Juvenile Offenders



Legal Recommendations: *Increasing Effectiveness of Federal Assurance Efforts*

GOAL: Improve Federal Government's Ability to Prevent & Mitigate, Reconstitute and Recover From Harm to Critical Infrastructures

- ➔ Reassess major federal legislation in light of infrastructure assurance concerns
 - Defense Production Act
 - study priorities in contract for use in post-event reconstitution and recovery
 - Stafford Act/Federal Response Plan
 - study appropriateness as response to cyber incidents, including desirability of providing direct assistance to owners and operators
 - Nunn-Lugar-Domenici
 - Consider expansion beyond WMD to other physical attacks on critical infrastructures, and appropriateness for cyber event



Legal Recommendations: *Enabling Private Sector Protective Action*

GOAL: Expand Private Sector's Ability to Counter Insider Threat Through Limited Use of Background Information When Hiring for Sensitive Positions

- ⇒ Convene expert study group to balance owner-operators' need to conduct background investigations with employees' privacy interests.
- Consider allowing some owners and operators to request from employees for sensitive positions information similar to that which is routinely be obtained by the federal government when issuing security clearances:
 - Criminal history information
 - Credit history information
 - Employment history



Legal Recommendations: *Enabling Private Sector Protective Action*

GOAL: Enable the Private Sector to More Confidently Hire Computer Security Personnel

- ➔ Extend laws governing providers of physical security to those who provide computer and information security
 - *For example:* extend exemption for physical security personnel in Employee Polygraph Protection Act to also cover computer security personnel





Legal Recommendations: *Reassessing Legal Impediments to Partnership*



GOAL: To Promote Formation of Effective Public-Private Partnership Where Needed for Infrastructure Assurance

- I. Address Legal Impediments to Public-Private Information Sharing
- II. Address Legal Impediments to Public-Private Policy Formulation



Legal Recommendations: *Reassessing Legal Impediments to Partnership*

GOAL:

To Create a Trusted Environment for Voluntary Sharing of Sensitive Threat and Vulnerability Information

- Private sector and private sector
- Government and government
- Government and private sector

Key Observation: To promote voluntary sharing of sensitive information, the government must demonstrate that information can be appropriately protected from unauthorized disclosure





Legal Recommendations: *Reassessing Legal Impediments to Partnership*

- ➔ **Creating a trusted environment for information sharing that adequately addresses legal impediments:**
- ***Antitrust***- offer limited assurances that participation in sanctioned information sharing processes will not run afoul of antitrust laws
 - ***Liability***- participants in sanctioned information sharing activities (including the government) should study liability consequences and specifically enumerate duties and obligations arising out of participation
 - ***National security***- participants in sanctioned information sharing activities should set guidelines for the sharing of threat and vulnerability information with foreign corporations or multinationals



Legal Recommendations: *Reassessing Legal Impediments to Partnership*

- ⇒ **Creating a trusted environment for information sharing that adequately addresses legal impediments:**
- ***Classified and proprietary information***- sanctioned information-sharing activities should derive informational value from, but continue to protect, classified and proprietary information
 - ***Access to government information***- sensitive information derived through sanctioned information sharing activities should be protected from disclosure under laws requiring public access to federal government information (e.g., FOIA)
 - ***State and local participation***- participation in sanctioned information sharing activities should not be precluded as a result of laws requiring public access to state government information

Legal Recommendations: *Reassessing Legal Impediments to Partnership*

GOAL:

To Create a Trusted Environment in Which to Promote Candid Policy Discussions Involving Sensitive Threat and Vulnerability Information

- ➔ Consider exemptions from public meeting requirements (e.g., FACA) for sanctioned public-private policy formulation discussions involving sensitive information about threats to and vulnerabilities of critical national infrastructures

