

# INFRASTRUCTURE PROTECTION SOLUTIONS CATALOG

A “LEGAL FOUNDATIONS” STUDY  
Report 5 of 12

Report to the  
President’s Commission  
on Critical Infrastructure Protection  
1997



This report was submitted to the President’s Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

---

---

# Contents

---

---

TABLE OF CONTENTS.....	ii
ACKNOWLEDGMENTS .....	iv
PREFACE.....	v
INTRODUCTION.....	vii
I. SOLUTIONS RELATING TO THE CREATION OF A NEW FEDERAL POLICY ENTITY .....	1
II. SOLUTIONS RELATING TO THE CREATION OF A FEDERAL COORDINATING ENTITY INCLUDING OPERATIONAL RESPONSIBILITIES (E.G. FUNDING AUTHORITY, RULEMAKING AUTHORITY).....	4
III. SOLUTIONS RELATING TO THE NEED FOR A PERMANENT “IPTF” CAPABILITY .....	7
IV. SOLUTIONS RELATING TO ENHANCEMENT OF PROTECTION, MITIGATION, RECOVERY AND EMERGENCY RESPONSE CAPABILITIES, INCLUDING DEVELOPMENT AND REFINEMENT OF COORDINATED EMERGENCY RESPONSE PLANS.....	10
V. SOLUTIONS RELATING TO THE IDENTIFICATION, CREATION AND MAINTENANCE OF A “MINIMAL ESSENTIAL INFRASTRUCTURE,” INCLUDING CRITICAL NODE IDENTIFICATION ...	13
VI. SOLUTIONS RELATING TO CREATION OF A CENTRALIZED DATA COLLECTION AND ANALYSIS CAPABILITY.....	14
VII. SOLUTIONS RELATING TO THE FEDERAL GOVERNMENT’S “MODEL” PERFORMANCE (I.E., INFLUENCING PRIVATE SECTOR BEHAVIOR THROUGH UNILATERAL EFFORTS AT INFORMATION SHARING, STANDARDIZATION AND PROCUREMENT) .....	16
VIII. SOLUTIONS RELATING TO EXISTING FEDERAL DEPARTMENT AND AGENCY JURISDICTION AND AUTHORITY.....	17
IX. SOLUTIONS RELATING TO ADMINISTRATIVE AND REGULATORY REQUIREMENTS FOR GOVERNMENT .....	19
X. SOLUTIONS RELATING TO JOINT PUBLIC-PRIVATE AND GOVERNMENT-ASSISTED RESEARCH, DEVELOPMENT AND TECHNOLOGY .....	21
XI. SOLUTIONS RELATING TO CERTIFICATIONS, STANDARDS AND GUIDELINES .....	26
XII. SOLUTIONS RELATING TO INFLUENCING EXISTING LIABILITY CLIMATES .....	29
XIII. SOLUTIONS RELATING TO ADMINISTRATIVE AND REGULATORY REQUIREMENTS FOR THE PRIVATE SECTOR.....	30
XIV. SOLUTIONS RELATING TO PUBLIC-PRIVATE INVESTMENT INCENTIVES .....	34

<b>XV. SOLUTIONS RELATING TO THE DEVELOPMENT OF NEW RISK MANAGEMENT MODELS..</b>	<b>35</b>
<b>XVI. SOLUTIONS RELATING TO PUBLIC AWARENESS AND EDUCATION.....</b>	<b>36</b>
<b>XVII. SOLUTIONS RELATING TO PROFESSIONAL TRAINING.....</b>	<b>40</b>
<b>XVIII. SOLUTIONS RELATING TO ENHANCING INTERNATIONAL COOPERATION AND PARTICIPATION IN ASSURANCE PRACTICES.....</b>	<b>42</b>
<b>XIX. SOLUTIONS RELATING TO EXPORT AND TRADE POLICY.....</b>	<b>44</b>
<b>XX. SOLUTIONS RELATING TO ENHANCING DETERRENCE.....</b>	<b>45</b>
<b>XXI. SOLUTIONS RELATING TO PERIOD OF TRANSITION TO WAR.....</b>	<b>46</b>
<b>XXII. SOLUTIONS RELATING TO GOVERNMENT AND CIVILIAN RESPONSIBILITIES IN TIME OF WAR (DECLARED WAR).....</b>	<b>47</b>
<b>XXIII. SOLUTIONS RELATING TO EXISTING LEGISLATION/REGULATIONS.....</b>	<b>48</b>
<b>XXIV. SOLUTIONS RELATING TO SHORT-TERM ASSURANCE MEASURES (LOW-HANGING FRUIT).....</b>	<b>50</b>
<b>BIBLIOGRAPHY.....</b>	<b>52</b>
<b>APPENDIX A:.....</b>	<b>A-1</b>

---

---

# Acknowledgments

---

---

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

---

---

# Preface

---

---

Executive Order 13010 established the President’s Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

*Legal Foundations: Studies and Conclusions* is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the possible approaches and conclusions that were presented to the PCCIP for its consideration. The

series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

---

---

# Introduction

---

---

**“Never hype a problem unless you have a solution.”** (*statement in a meeting with Commissioners and staff of the President’s Commission on Critical Infrastructure Commission*)

**Michael R. Nelson, Director, Technology Policy  
Office of Plans and Policy  
Federal Communications Commission**

In early 1997, the requirement arose in the President’s Commission for Critical Infrastructure Protection (PCCIP) for maintaining a running catalog of ideas relating to potential solutions for infrastructure protection. In assembling this catalog, we relied heavily on the work of other bodies that preceded the President’s Commission. The *Infrastructure Protection Solutions Catalog* embodied those preliminary efforts and was maintained through March 1997, the time at which the Commission began to formulate its own potential recommendations. It is a compendium of prior recommendations made by informed individuals, study commissions, and other groups who have weighed in on issues related to infrastructure assurance.

Possible solutions are arranged within broad solution categories. Within each category is a general description of its scope and an “external considerations” section. External considerations are specific solution-related ideas, proposals or recommendations that came to our attention by way of the papers and briefings referenced in the Bibliography to this document.

These efforts led to the development of another "Solutions Catalog" used during the U.S. Infrastructure Assurance Prosperity Game and Planning Event Number 2, held on March 23-25, 1997 in Chantilly, Virginia. The event was sponsored by the President's Commission on Critical Infrastructure Protection, the National Communications System and the Department of Energy, and was produced by Sandia National Laboratories and the Prosperity Institute. This catalog is also included here in Appendix A, as it appeared in gaming materials, to demonstrate the full range of solution ideas that were brought to the attention of the PCCIP to inform its deliberations

# I. SOLUTIONS RELATING TO THE CREATION OF A NEW FEDERAL POLICY ENTITY

## Coordinate Public/Private Assurance Efforts

This category encompasses solutions aimed at creating an entity to carry on the work of the PCCIP. This entity could take the form of an executive branch agency, a Federal spokesperson or “czar” model, an independent regulatory commission (created by Congress), or a standing executive branch advisory committee. The scope of the entity’s authority could include the full range of critical infrastructures, as well as the ability to leverage Cabinet-level agency resources. Private sector participation, substructures within the entity for each critical infrastructure, and the appropriate level of staffing are all issues that will need to be considered.

### External Considerations

Establish a joint office for system, network and infrastructure design to promote utility, resiliency, reparability and security in infrastructures.	(Defense Science Board Task Force on Information Warfare-Defense, November 1996).
Reduce the expectation of an all-encompassing response from the Department of Defense.	(Logan, Michael; 5 <sup>th</sup> International Conference on Information Warfare, 1996).
Need effective collaboration between the federal national security community and private sector industries because of the degree of dependence of the government on privately provided transportation, telecommunications and energy.	(Volpe Center).
Establish an Information Security Foundation.	(National Research Council, “Computers at Risk,” 1991).

Stand up an Information Assurance Committee (IAC) under the PDD-29 Security Policy Board structure to create information assurance policy for Government systems processing classified and national security information. The IAC would also propose legislation, policy, and regulations for the Executive branch and influence private and non-government entities important to national security. <sup>1</sup>	(U.S. Security Policy Board, "White Paper on Information Infrastructure Assurance," 1996).
Broaden NSTAC's charter to reflect the full scale of NII issues beyond telecommunications, security and national security.	(U.S. Security Policy Board, "White Paper on Information Infrastructure Assurance," 1996).
Establish an Information Assurance focus within the National Security Council.	(U.S. Security Policy Board, "White Paper on Information Infrastructure Assurance," 1996).
Assign a focal point for Federal government leadership in support of a coordinated U.S. response to the strategic IW threat. Also conduct risk assessments, discuss proper government role, address preparedness.	(RAND, "Strategic Information Warfare: A New Face of War," 1996).
Create an NSTAC-like advisory committee for the electric power industry.	(NSTAC Information Assurance Task Force, "Electric Power Information Assurance Risk Assessment," 1996).
Establish individual infrastructure sector advisory committees, based on the NSTAC model, to facilitate communication and information sharing and generate policy recommendations.	(Center for Strategic International Studies (CSIS) Information Assurance Working Group, internal PCCIP memo by Commissioner Brenton Greene dated October 2, 1996).
Advances need to be made in the following policy areas: <ul style="list-style-type: none"> <li>• achieving consensus on problems and solutions</li> <li>• enhancing government/industry cooperation for identifying and characterizing reliability challenges</li> <li>• enhancing Federal and state interaction to ensure consistent and appropriate attention is placed on infrastructure reliability</li> </ul>	(OSTP, "Cybernation," Draft of January 17, 1997).
Devise an integrated program combining security technology, managerial practices, and US government policy into a mutually supporting coherent program for the protection of U.S. financial institutions.	(Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997).

---

<sup>1</sup> May require replacing or modifying PL 100-235, NSD-42, OMB Circular A-130, Paperwork Reduction Act, and other subordinate directives.

## **Identify and Leverage Sources of Funding for Public/Private Assurance Efforts**

---

This subsection will be used to catalog potential sources of funding that can be used to build and maintain the entities and capabilities described in items I-III. The range of possibilities for funding may include earmarking a certain percentage of available funds expressly for assurance efforts or recommending that state and local governments identify and develop similar funding sources, “matching” or incentive programs to further assure infrastructures deemed critical to their own sustained operations.

## II. SOLUTIONS RELATING TO THE CREATION OF A FEDERAL COORDINATING ENTITY INCLUDING OPERATIONAL RESPONSIBILITIES (E.G. FUNDING AUTHORITY, RULEMAKING AUTHORITY)

### “Manager” of Interagency Indications and Warning Capability

Solutions under this category address creation of a capability for coordinating and maintaining a nationwide indications and warnings system. Such a capability should allow for the exchange of appropriate information with the private sector and federal, state and local governments, including the intelligence and law enforcement communities. It may also include an appropriate international liaison capability. It could also serve as a repository for the operational resources (personnel, equipment, etc.) that would comprise the Federal government’s emergency response and response management capabilities described in the next section. This “manager” may also be able to assume many of the responsibilities currently delegated to the Infrastructure Protection Task Force (IPTF) by E.O. 13010.

#### External Considerations

Create a center for intelligence indications and warnings, current intelligence and threat assessments within NSA.	(Defense Science Board Task Force on IW-D, 1996).
Create a center for information warfare defense operations within DISA, to have links with any successor of the IPTF.	(Defense Science Board Task Force on IW-D, 1996).
Create a National Information Infrastructure Threat Center with representatives from law enforcement, intelligence and the Defense communities to perform liaison with the private sector, act as a clearinghouse for intrusion reports, and have “real time” 24-hour operational capabilities.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).

Promote regular vulnerability assessments, or “red teaming,” of government agencies, especially those outside of the Department of Defense, to operate in a manner similar to that of DISA in assessing the armed forces.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Establish an early warning capability that uses internet messages to help identify developing situations overseas that could lead to security threats.	(Swett, Charles, OSD; “Strategic Assessment: The Internet,” 1995).
Use a flexible integrated response to counter information terrorists, employing information warfare tactics tailored to countering gray-area phenomena, but also reserving the use of conventional counter-terrorism operations.	(Devost, Houghton, & Pollard, “Information Terrorism: Can You Trust Your Toaster?,” 1996).
Response structure should incorporate assets from both the military and law enforcement. The military should take an advisory role in domestic incidents, and law enforcement assets a similar role in overseas incidents.	(Devost, Houghton, & Pollard, “Information Terrorism: Can You Trust Your Toaster?,” 1996).
Establish mechanisms to support focused information exchange, provide information on threats, vulnerabilities and mitigation measures, and to facilitate identification of recommended actions by industry and government to ensure the viability and security of the National Information Infrastructure (NII).	(Information Infrastructure Task Force, “NII Risk Assessment: A Nation’s Information at Risk,” 1996).
Facilitate the inclusion of NII risk data in other relevant data collection activities, such as those conducted by the Census Bureau or the National Economic Council.	(Information Infrastructure Task Force, “NII Risk Assessment: A Nation’s Information at Risk,” 1996).
Establish a red team for independent assessments of vulnerabilities.	(Defense Science Board Task Force on IW-D, 1996).
Establish a method to facilitate the flow of intrusion and threat data between and among government agencies, especially law enforcement and intelligence communities, and the private sector. Mechanism should include a process to provide effective threat warnings and pattern analysis to aid in the protection and assurance of information and information-based control systems.	(CSIS Information Assurance Working Group, PCCIP Commissioner Greene memo dated October 2, 1996).
Establish a new agency in the Executive Office of the President to address Information Assurance. Functions of the agency would include review, coordinate, propose, and, where appropriate, direct Executive Branch NII protection-related policy, resource allocation, education, training and awareness, legislation, technology development and application, international liaison, and threat/vulnerability assessment.	(U.S. Security Policy Board, “White Paper on Information Infrastructure Assurance,” 1996; SPB Briefing to Commission, September 23, 1996).

<p>Establish a NII Threat Center with 24 hour, 7 days a week operations.</p>	<p>(Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997).</p>
<p>Create a national process for strategic information warfare threats Indications and Warnings to include the following features:</p> <ul style="list-style-type: none"> <li>• dual track watch centers to monitor IW indicators, infrastructure status and intrusion patterns</li> <li>• reporting channels to communication information between two tracks</li> <li>• centralized warning function</li> <li>• reporting channels to communication warnings to key decision makers</li> <li>• IW threat management process</li> <li>• standing National Security and Emergency Coordination (NS/EP) programs for strategic IW threat</li> <li>• mechanisms to integrate offensive skills into defense programs</li> <li>• national level test and exercise regimes.</li> </ul>	<p>(NSR, "Indications and Warnings of Strategic Information Warfare," October 1996).</p>

# III. SOLUTIONS RELATING TO THE NEED FOR A PERMANENT “IPTF” CAPABILITY

Solutions in this category address whether certain functions are set out in Executive Order 13010 that are not captured in the operational entity discussed in the category above. This category contemplates creation of an ongoing IPTF (Infrastructure Protection Task Force) capability to fill these needs.

## Issue Threat and Warning Notices

Solutions relating to a threat and warning capability are closely related to the solutions relating to the creation of an indications and warnings “manager.” Solutions falling under this subsection relate specifically to placing that capability under the purview of a permanent IPTF capability. These solutions will include a broad range of ideas that vary according to the amount of private sector and law enforcement involvement.

### External Considerations

Create a center for intelligence indications and warnings, current intelligence and threat assessments within NSA.	(Defense Science Board Task Force on IW-D, 1996).
Create a National Information Infrastructure Threat Center with representatives from law enforcement, intelligence and defense communities to perform liaison with the private sector, act as a clearinghouse for intrusion reports, and have “real time” 24-hour operational capabilities.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996). See also, Nickson, Mark, “Vulnerability of US Financial Markets to an Information Warfare Attack,” Draft of March, 1997. Software Publishers Association (SPA) also supports creation of a clearinghouse.

Promote creation of an international computer crime bureau with emergency response capability.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Secretary of Energy should establish within the Department of Energy a focal point for energy security matters and make it responsible for collecting relevant intelligence information from cognizant government agencies and providing the petroleum industry with advance warnings of potential dangers.	(Comptroller General Report to Congress, 1979).
Establish and staff a national-level NII operations center within the Executive Office of the President (or National Security Council (NSC), or Federal Emergency Management Agency (FEMA)) to execute national 24/7 operational indications and warnings, detection/assessment, and reaction functions.	(SPB Briefing to the PCCIP, September 23, 1996).
Create new legislation to provide for monitoring critical parts of the NII for National Infrastructure Assurance purposes with built in safeguards to prevent government abuse.	(SPB Briefing to the PCCIP, September 23, 1996).
Share threat information available to the government with the private sector.	(CERT Coordination Center, Report to PCCIP, January 1997).
Support the growth and use of global detection mechanisms by using incident response teams to identify new threats and vulnerabilities.	(CERT Coordination Center, Report to PCCIP, January 1997).
Create an equitable, institutional means, with clear statutory boundaries, for the timely two-way flow of relevant intelligence information and incident data between government and private utilities, which protects business-sensitive data as well as sources and methods. This institution, which would bring government and industry together, would provide early warning of hostile activities.	(OSTP, "Cybernation," draft of January 17, 1997).
Establish threat response teams of technical experts, system operators, and law enforcement officials to respond to requests from infrastructure operators. Teams may be ad hoc, but small permanent organization needs to refine response process, coordinate action and advise system operators.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

## Provide Training and Education on Reducing Vulnerabilities and Responding to Attacks

---

This category will capture solutions relating to creation of an ongoing training and education role for a follow-on IPTF capability.

### External Considerations

---

Create an international computer crime bureau to provide education and awareness to foreign law enforcement agencies in order to promote the creation of dedicated computer crime units as well as uniform investigative and computer forensic practices.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Promote regular vulnerability assessments, or “red teaming,” of government agencies, especially those outside of the Department of Defense, to operate in a manner similar to that of DISA in assessing the armed forces.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Federal government should work with public and private infrastructure operators in planning and executing simulations, tests, and exercises to help identify vulnerabilities, attack signatures and defensive concepts. This should be jointly funded.	(Lukasik, Steve; “Public and Private Roles in the Protection of Critical Infrastructure,” March 1997).

## Provide/Facilitate Provision of Expert Guidance to a Halt or Confine Attack and Restore Service

---

### External Considerations

---

Create a center for information warfare defense operations within DISA, to have links with any successor of the IPTF.	(Defense Science Board Task Force on IW-D, 1996).
Establish a national coordinating and response center, and individual response centers for each of the infrastructure sectors, to facilitate consequence management and capability restoration.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).

# IV. SOLUTIONS RELATING TO ENHANCEMENT OF PROTECTION, MITIGATION, RECOVERY AND EMERGENCY RESPONSE CAPABILITIES, INCLUDING DEVELOPMENT AND REFINEMENT OF COORDINATED EMERGENCY RESPONSE PLANS

## Federal

Solutions in this category propose means of enhancing the nation’s emergency response mechanisms including protection, mitigation and recovery efforts. Solutions could include changes to the Federal Response Plan such as changing definitions to address cyber issues, greater use of mitigation tactics, and appropriate funding. All solutions will need to adequately consider the need for prioritization in the event of an emergency, as well as clear delineation of responsibilities among interested parties.

### External Considerations

Expand the definition of disaster to include information warfare and expand recovery mechanisms to prepare for and recover from information disasters.	(Logan, Michael; 5 <sup>th</sup> International Conference on Information Warfare, 1996).
Need for clearer policy assigning responsibilities for coordinating emergency actions to deal with threats to water quality.	(U.S. Congress, “Water Quality: A Catalog of Related Federal Programs.”).
Recommendations regarding development of emergency plans for telecommunications: <ul style="list-style-type: none"> <li>• establish a Nationwide Emergency Telecommunications Service</li> <li>• deploy NCS and FCC priority service through industry for use in declared emergencies</li> </ul>	(National Research Council, “Growing Vulnerability of the Public Switched Networks,” 1989).

<ul style="list-style-type: none"> <li>• add route diversity and node diversity</li> <li>• increase radio access capabilities through either terrestrial or satellite radio transmission</li> <li>• use simulated disaster and recovery scenarios to develop strategies for network use during emergencies</li> <li>• establish software security measures to protect public network from penetration by hostile users</li> <li>• exploit value-added networks</li> <li>• promote inter-network gateways.</li> </ul>	
<p>Assure adequate emergency response capability on the National Information Infrastructure.</p>	<p>(Information Infrastructure Task Force Security Issues Forum, “NII Security: The Federal Role,” 1996).</p>
<p>Improve national security/emergency preparedness capabilities.</p>	<p>(Information Infrastructure Task Force Security Issues Forum, “NII Security: The Federal Role,” 1996).</p>
<p>Flexible, automated, prioritized responses to disruption should be implemented:</p> <ul style="list-style-type: none"> <li>• design the Defense Information Infrastructure for automated detection, differentiation, warning, response, and recovery from disruptions</li> <li>• design data centers, network components, and network control centers for ease of repair.</li> </ul>	<p>(DISA, “Planning Considerations for Defensive Information Warfare- Information Assurance,” 1993).</p>
<p>Increase robustness of U.S. infrastructure systems.</p>	<p>(RAND, “Risks to the U.S. Infrastructure from Cyberspace,” 1996).</p>
<p>Army should review legal constraints on military participation in civil disaster relief.</p>	<p>(Schrader, K.J.; “The Army’s Role in Domestic Disaster Support: An Assessment of Policy Choices,” 1993).</p>
<p>Army should support formal acceptance of civil disaster response as a mission for both active and reserve forces.</p>	<p>(Schrader, K.J.; “The Army’s Role in Domestic Disaster Support: An Assessment of Policy Choices,” 1993).</p>
<p>The Secretary of Energy should establish contingency plans for minimizing supply shortages which could result from prolonged disruptions in the flow of petroleum through important pipeline systems.</p>	<p>(Comptroller General Report to Congress, 1979).</p>

Create a stockpile of transformers beyond the level of normal spares or require utilities to back up each important transformer.	(U.S. Congress, Office of Technology Assessment, "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage," 1990).
Establish and advertise national policies for protection of vital infrastructures and promulgate strategies for deterring structured attacks.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Assess current federal emergency preparedness for inter-jurisdictional gaps and overlaps; adequacy to deal with network risks and organization of FEMA through creation of a Congressional Joint Committee.	(CSIS, "America's Hidden Vulnerabilities: Crisis Management in a Society of Networks," 1984).
Congress should fund an inter-industry Emergency Preparedness Council of industry and academic representatives to provide an industry-government interface and serve as a pilot instrument for private sector cooperation in emergency planning and the setting of standards.	(CSIS, "America's Hidden Vulnerabilities: Crisis Management in a Society of Networks," 1984).
Create a set of emergency restart sites for re-establishing networks after an Internet failure.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).

## State

---

Solutions relating to state enhancement of protection, mitigation, recovery and response to emergency situations could cover a broad range of activities based on availability of resources and state cooperation. A model disaster recovery statute is one solution with a modest amount of federal resources and involvement required; however additional solutions, such as creating incentives for enhancing existing state plans, may also be considered.

## V. SOLUTIONS RELATING TO THE IDENTIFICATION, CREATION AND MAINTENANCE OF A “MINIMAL ESSENTIAL INFRASTRUCTURE,” INCLUDING CRITICAL NODE IDENTIFICATION

### External Considerations

Identify the elements and processes of national information, both public and privately owned which collectively comprise the “vital national information interests.” Such interests should include both physical infrastructure components and virtual processes, capabilities, and some forms of information.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Create a minimum essential information infrastructure for use in restoring services and adapting to wide-scale outages.	(Defense Science Board Task Force on IW-D, 1996).
Make investments to protect key electrical system facilities, particularly substations. Base levels of protection on importance, physical characteristics, location and the nature of the threat.	(U.S. Congress, Office of Technology Assessment, “Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage,” 1990).
Establish and advertise national policies for protection of vital infrastructures and promulgate strategies for deterring structured attacks.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Revisit FEMA’s proposed National Asset Program.	(U.S. Senate Subcommittee on Governmental Affairs, “Draft Committee Report on Network Vulnerabilities to Terrorist Attack, 1989).
Consider advisability and feasibility of creating a minimum essential information infrastructure.	(RAND, “Risks to the U.S. Infrastructure from Cyberspace,” 1996).

# VI. SOLUTIONS RELATING TO CREATION OF A CENTRALIZED DATA COLLECTION AND ANALYSIS CAPABILITY

## Government (Federal)

### External Considerations

<p>Create an information clearing house and analytical activity with authority to task all Executive Branch elements to provide it with information; to accept information from other government agencies and to develop retrievable system of records; to deal with and protect information at all classification levels (to receive proprietary information from private sector without being subject to FOIA); to create a staff of analytical and substantive experts from all elements of government on a reimbursable basis; to disseminate its analytical products.</p>	<p>(Keyes, David; “Stove-Pipe City: It’s Not a New Computer Game, It’s Why Infrastructure Assurance Needs Centralized Analysis,” October 17, 1996).</p>
<p>Create an interim clearing house capability using either the IPTF or the Joint Intelligence Community Law Enforcement process.</p>	<p>(Keyes, David; “Stove-Pipe City: It’s Not a New Computer Game, It’s Why Infrastructure Assurance Needs Centralized Analysis,” October 17, 1996).</p>
<p>Establish a method to facilitate the flow of intrusion and threat data between and among government agencies, especially law enforcement and intelligence communities, and the private sector. Mechanism should include a process to provide effective threat warnings and pattern analysis to aid in the protection and assurance of information and information-based control systems.</p>	<p>(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).</p>
<p>Congress should support the interface of selected civil and military agency resource databases and crisis control systems with White House systems for emergency coordination.</p>	<p>(CSIS, “America’s Hidden Vulnerabilities: Crisis Management in a Society of Networks,” 1984).</p>

<p>Refocus National Computer Emergency Response Teams and other incident collection centers to collect data not now collected on what information resources or services supporting critical infrastructures were impacted or affected. Need to guarantee absolute confidentiality to facilitate reporting of computer intrusions from the private sector.</p>	<p>(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).</p>
<p>Designate a single, independent, trusted organization to be responsible for collecting, analyzing, and reporting incident data. Organization should be neither government nor commercial and should not have other responsibilities such as public policy, investigation, or enforcement.</p>	<p>(CERT Coordination Center, Report to PCCIP, January 1997).</p>
<p>Create an equitable, institutional means, with clear statutory boundaries, for the timely two-way flow of relevant intelligence information and incident data between government and private utilities, which protects business-sensitive data as well as sources and methods.</p>	<p>(OSTP, "Cybernation," draft of January 17, 1997).</p>
<p>Encourage private industry to create an anonymous clearinghouse to allow businesses to report attacks while maintaining privacy.</p>	<p>(Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997).</p>
<p>Establish a point within the Federal government for system owners and operators to report threats to infrastructure. May be parallel structure in private industry. Reporting of threats to federal systems needs to be mandatory.</p>	<p>(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).</p>

**VII. SOLUTIONS RELATING TO THE  
FEDERAL GOVERNMENT’S “MODEL”  
PERFORMANCE (I.E., INFLUENCING  
PRIVATE SECTOR BEHAVIOR  
THROUGH UNILATERAL EFFORTS AT  
INFORMATION SHARING,  
STANDARDIZATION AND  
PROCUREMENT)**

Solutions in this category suggest means by which the Federal government can promote infrastructure assurance objectives through unilateral changes to its own practices. Solutions relate to both role of the government as model user and specific security measures that should be adopted in that role.

**External Considerations**

Government has the responsibility to act as a model user by protecting information in its possession and its own security requirements through good management processes.	(Information Infrastructure Task Force Security Issues Forum, “NII Security: The Federal Role,” 1996.)
The government should lead by example in achieving a robust and secure information environment by demonstrating a will to purchase and implement products and practices that promote system security.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
DoD should design a curriculum for the study of cyber security including system design, detection of intrusion, intrusion response, firewall design and implementation, and so on. Curriculum could form a new category of engineering in the military academics of an Associates Degree from the Industrial College of the Armed Forces.	(Commissioner Keyes memo, November 6, 1996).

## VIII. SOLUTIONS RELATING TO EXISTING FEDERAL DEPARTMENT AND AGENCY JURISDICTION AND AUTHORITY

This category collects solutions suggesting that clearer boundary lines, or new boundary lines, be drawn to delineate jurisdiction and responsibilities between existing federal government entities, including the law enforcement, intelligence, and defense communities.

### External Considerations

Roles and missions among those responsible for security must be clarified and coordinated.	(RAND, "Risks to the U.S. Infrastructure from Cyberspace," 1996).
Congressional oversight is needed to ensure top-management involvement in security, refocusing federal policy activity on technology neutral policy, and determining where federal authority for safeguarding unclassified information in the civil agencies should reside.	(U.S. Congress, Office of Technology Assessment, "Issue Update on Information Security and Privacy in Network Environments," 1995).
Explore the manner in which the responsibilities levied by E.O. 12656 will be implemented since federal agencies do not have the authority to require cooperation of the owner of a private asset designated as a key facility.	(U.S. Subcommittee on Governmental Affairs, Draft Committee Report on Network Vulnerabilities to Terrorist Attack, 1989).
Clarification of the missions, responsibilities, and authorities of national defense, intelligence, and law enforcement are needed for dealing with cyberspace threats. This will involve all three branches of government.	(OSTP, "Cybernation," Draft of January 17, 1997).
Federal government should address its own complex organization and settle jurisdictional issues for responding to infrastructure threats.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

## Law Enforcement Community

---

### External Considerations

---

Examine the proper role of law enforcement in policing the online world.	(German, Jerry; Testimony on the right to free speech, free association, and privacy on the Internet in the aftermath of Oklahoma City, Subcommittee on Terrorism, Technology, and Government Information, 1995).
Maintain cautious interpretation of Attorney General's guidelines for online investigations.	(German, Jerry; Testimony on the right to free speech, free association, and privacy on the Internet in the aftermath of Oklahoma City, Subcommittee on Terrorism, Technology, and Government Information, 1995).
Treat proposals to expand surveillance authority with great caution so that protection efforts do not infringe upon civil liberties.	(German, Jerry; Testimony on the right to free speech, free association, and privacy on the Internet in the aftermath of Oklahoma City, Subcommittee on Terrorism, Technology, and Government Information, 1995).

## IX. SOLUTIONS RELATING TO ADMINISTRATIVE AND REGULATORY REQUIREMENTS FOR GOVERNMENT

Solutions in this category will address whether government-wide administrative and regulatory requirements, such as mandatory reporting of significant intrusion incidents, would contribute substantially toward achieving an effective indications and warnings system, or whether an expanded program of voluntary compliance would provide sufficient data. Solutions will also address the appropriate vehicles for promulgation and enforcement of such administrative or regulatory requirements including whether agencies should promulgate and enforce their own regulations to comport with government standards, or whether such regulations should be promulgated and enforced by either of the entities proposed above. Solutions could take the form of recommendations regarding mandatory encryption of Supervisory Control And Data Acquisition system (SCADA), information, use of certified intrusion detection systems, or specified reserve capacities or redundancy margins.

### External Considerations

Create Government Computer Security Specialist and Computer Systems Administrator Career Fields with potential for career progression and incorporate specialized computer security training.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996). Concur. (Defense Science Board Task Force on IW-D, 1996).
Mandate the reporting of intrusions and attempted intrusions in government and government interest systems. Federal agencies should develop protocols and procedures for reporting computer intrusions and for referral to appropriate criminal and other agencies.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Make logon warning banners mandatory for all government and government interest systems.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).

Protect system from information warfare (IW) attacks using firewalls, enhanced domain compartmentalization, controlled transfer between domains; with monitoring and probing tools, deploying network administration/management, real-time monitoring, and reactive capability; and embedded encryption.	(Naval Research Advisory Council (NRAC) Study, 1996).
Address the vulnerabilities of military use of commercial SATCOM systems that provide geolocation and develop technology and operating procedures to minimize the impact of denial of service and avoid geolocation.	(Naval Research Advisory Council (NRAC) Study, 1996).
Make IW-D a higher priority by including it as part of exercises, doing operational analysis, and designating IW-D as an acquisition reform model to reduce time to achieve operational capability.	(Naval Research Advisory Council (NRAC) Study, 1996).
Create a capability for detection and early warning of cyber attacks on systems. Consider using a screening process similar to that used for airline passenger for the cyber arena; a screening process to filter out malicious code as it passes through telephone switches; adapting current tools for indications and warnings purposes.	(Commissioner Keyes memo, December 16, 1996).
Legislate for mandatory reporting of Information Warfare attacks in the public sector.	(Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997).

## **Federal (Defense Community)**

---

### **External Considerations**

---

Create a Government Computer Crime Investigators Career Field that includes potential for career progression and specialized computer crime training.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Consider the proper role of the federal government in guaranteeing the reliability of interstate energy distribution and telecommunications networks, to the extent it is beyond the capability of individual states.	(U.S. Senate Subcommittee on Governmental Affairs, Draft Committee Report on Network Vulnerabilities to Terrorist Attack, 1989).

## **X. SOLUTIONS RELATING TO JOINT PUBLIC-PRIVATE AND GOVERNMENT- ASSISTED RESEARCH, DEVELOPMENT AND TECHNOLOGY**

Research and development solutions in this category take three basic forms. Solutions may suggest topics in need of research and development; forms of government, government-private cooperative, or purely private research and development initiatives; or incentives or mechanisms to encourage research and development within the recommended areas. Options may include the funding and establishment of a government subsidized industrial institute; Congressionally approved Cooperative Research and Development Authorities (CRADAs); or expansion of the existing capabilities of the National Labs to provide partially subsidized research services for qualified assurance-related projects.

### **Areas of Study**

#### **External Considerations**

Fund and pursue needed research on computer and communications security.	(National Research Council, "Computers at Risk," 1991).
Federal Government should promote research and development in critical and high-risk areas.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996.)
Real-time control mechanisms to enhance information assurance should be developed.	(DISA, "Planning Considerations for Defensive Information Warfare- Information Assurance," 1993).

Focus research and development on robust survivable system architectures; techniques and tools for modeling, monitoring, and management of large-scale distributed/network systems; tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks; and tools and techniques for automated detection and analysis of localized or coordinated large scale attacks.	(Defense Science Board Task Force on IW-D, 1996).
Set a national agenda and prioritize research and development in information technology security, computer security and computer investigative fields to safeguard national infrastructures.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Government should create a capability for detection and early warning of cyber attacks on systems. Consider using a screening process similar to that used for airline passengers in the cyber arena; a screening process to filter out malicious code as it passes through telephone switches; adapting current tools for indications and warnings purposes.	(Commissioner Keyes memo, December 16, 1996).
Create testing programs to enhance information assurance.	(DISA, "Planning Considerations for Defensive Information Warfare-Information Assurance," 1993).
Government should fund a demonstration project to examine the costs, benefits and pitfalls of attempting to use encryption and authentication to prevent unauthorized access to SCADA control systems.	(Commissioner Keyes memo, December 16, 1996).
Fund research and development in areas of security and survivability of unbounded systems' architectures with distributed control.	(CERT Coordination Center, Report to PCCIP, January 1997).
Encourage the development of comprehensive system/security administrators' toolkits.	(CERT Coordination Center, Report to PCCIP, January 1997).
Support the development of techniques for comprehensive, continuous risk identification and mitigation programs.	(CERT Coordination Center, Report to PCCIP, January 1997).
Develop and strengthen tools and procedures for detecting, reporting and reacting to network problems.	(OSTP, "Cybernation," Draft of January 17, 1997).
Construct profiles of attack sources to develop a better understanding of attacker motivations and goals in order to develop better search parameters for them.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).
Develop technology to identify and collect information about a potential attacker while they are probing the system.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

Public infrastructure operators should take the responsibility for developing protection for those systems and to stimulate the transfer of that technology to the private sector.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).
Government infrastructure operators should test commercial audit system products and publish the results. Government would act as a test bed for new technology. A joint industry-government working group could be established to set requirements for system audits and provide information on the state of the technology.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

## **Bodies to Engage in Study (Government)**

---

### **External Considerations**

---

Federal government must support the needs of industry by supporting research and development.	(NSTAC, "An Assessment of the Risk to the Security of the Public Network," 1995).
Government should closely coordinate research and development within the government to avoid duplication of efforts and ensure that all critical areas are being addressed.	(Commissioner Keyes memo, December 16, 1996).

## **Bodies to Engage in Study (Joint Government-Private)**

---

### **External Considerations**

---

Fund national laboratories and government agencies and encourage academic and commercial participation.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Work with National Science Foundation to develop research in U.S. computer science and computer engineering programs and educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices.	(Defense Science Board Task Force on IW-D, 1996).

Government should support joint R&D with infrastructure operators and industry for information infrastructure defense.	(Lukasik, Steve; “Public and Private Roles in the Protection of Critical Infrastructure,” March 1997).
--	--

## **Bodies to Engage in Study (Private)**

---

### **External Considerations**

---

Industry should significantly increase its involvement with the university community and support academic research with grants, joint R&D projects, equipment, and fellowships.	(Center for Strategic and International Studies, “R&D for National Strength,” 1982).
Industry should utilize and encourage academic and governmental technology-transfer programs.	(Center for Strategic and International Studies, “R&D for National Strength,” 1982).
Academe should provide support and encouragement for those who work in military R&D and inculcate attitudes of risk-taking, innovation, and creativity among engineering and science students.	(Center for Strategic and International Studies, “R&D for National Strength,” 1982).
Academe should increase part-time academic positions for industrial, governmental and military R&D personnel.	(Center for Strategic and International Studies, “R&D for National Strength,” 1982).

## **Incentives**

---

### **External Considerations**

---

Congress assess whether amendment or reinterpretation of anti-trust legislation would encourage the organization of private sector industrial combinations and consortia strong enough to address major research and develop issues with their own resources.	(Center for Strategic and International Studies, “R&D for National Strength,” 1982).
Congress should use educational subsidies to encourage development of disciplines and research that contribute to military needs.	(Center for Strategic and International Studies, “R&D for National Strength,” 1982).

Congress should create new tax incentives to encourage major stimulation of the U.S. R&D industrial base and long-term investment in science and technology.	(Center for Strategic and International Studies, "R&D for National Strength," 1982).
Terms of procurement contracts should be changed to allow commercial market rights to government contractors as an incentive to private developers and to facilitate technology transfer to the private sector.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

# XI. SOLUTIONS RELATING TO CERTIFICATIONS, STANDARDS AND GUIDELINES

Solutions under this category will relate to the broad range of options for government or private sector action in setting standards or creating certifications for products or services that enhance assurance or assurance-related capabilities. Factors to be considered in formulating individual solutions should be the use of existing standard setting vehicles in the federal government such as NIST or NSA, interaction with other areas of concern for the Commission such as insurance and liability issues, and funding issues, and the need for monitoring and sanctions to ensure continued compliance with standards.

## External Considerations

Create a Government Computer Security Specialist and Computer Systems Administrator Career Fields with potential for career progression and incorporate specialized computer security training.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Promulgate comprehensive generally accepted system security principles, as well as methods, guidelines, and facilities for evaluating products for conformance.	(National Research Council, "Computers at Risk," 1991).
Manufacturers must ensure that the security capabilities of their goods and services adequately reflect the needs of the marketplace.	(NSTAC, "An Assessment of the Risk to the Security of the Public Network," 1995).
Users must subscribe to and pay for appropriate levels of privacy and security.	(NSTAC, "An Assessment of the Risk to the Security of the Public Network," 1995).
Government has the responsibility to protect information in its possession and protect its own security requirements through good management processes.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996.)
Telecommunications carriers should review their implementation of best practices to insure that alarms are in place and maintained, and that an effective alarm strategy is in place to promptly identify and address power problems.	(Alliance for Telecommunications Industry Solutions-Network Reliability Steering Committee (ATIS-NRSC), "Analysis of Power Related Network Outages," 1996).

Information assurance standards, technologies, tools, and guidelines should be developed.	(DISA, "Planning Considerations for Defensive Information Warfare- Information Assurance," 1993).
Design products flexible enough to serve a broad spectrum of security needs at the operating system level, the application level, the organizational level, and the site level.	(NIST, "Assessing Federal and Commercial Information Security Needs," 1992).
Vendors should consider new mechanisms that directly address discretionary and non-discretionary controls, such as role-based access controls, separation of duties, separation of transactions, and user-oriented least privilege.	(NIST, "Assessing Federal and Commercial Information Security Needs," 1992).
Secretary of Energy should establish minimum security standards for critical pipelines and related facilities.	(Comptroller General Report to Congress, 1979).
Establish an industry-wide standard for reliability reporting, analogous to the financial accounting and reporting guidance of the Financial Accounting Standards Board, for infrastructure operators. Board would help put discipline into the process of capturing and applying lessons learned.	(OSTP, "Cybernation," Draft of January 17, 1997).
Establish legitimized, generally accepted, and broadly applicable standards for network design and installation for enhanced reliability. The National Fire Protection Agency's National Electrical Code can be used as a model.	(OSTP, "Cybernation," Draft of January 17, 1997).
Develop institutionalized product reliability testing and certifications, similar to Underwriters Laboratories, for network components. Such certifications or testing would be of "immense value" for comparing products. Certifications or standards would ideally be created by a joint government-private sector effort.	(OSTP, "Cybernation," Draft of January 17, 1997).
Federal government could license and certify routes for the Internet and collateral attributes such as topography and survivability.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).
Federal government license and certify ISPs and related service providers based on quality, performance and security.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).
All networks should authenticate routing.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).
Private sector should develop voluntary, industry-wide, accepted best practices for information security. Government should support industry in this effort as requested, but especially in gaining support in the international arena for such practices.	(Copeland, Guy; "Information Assurance Insurance," February 1997).

<p>Government set standards need to be closely aligned with commercial and consumer interests to be effective.</p>	<p>(Neumann, Peter; “Security Risks in the Emerging Infrastructure,” Senate Testimony June 1996).</p>
<p>Regulators of infrastructure systems should take primary responsibility for encouraging their industries to take cooperative action through existing administrative procedures for the setting of standards.</p>	<p>(Lukasik, Steve; “Public and Private Roles in the Protection of Critical Infrastructure,” March 1997).</p>
<p>Government infrastructure operators should test commercial audit system products and publish the results. Government would act a test bed for new technology. A joint industry-government working group could be established to set requirements for system audits and provide information on the state of the technology.</p>	<p>(Lukasik, Steve; “Public and Private Roles in the Protection of Critical Infrastructure,” March 1997).</p>

## XII. SOLUTIONS RELATING TO INFLUENCING EXISTING LIABILITY CLIMATES

### External Considerations

Determine priorities in a natural emergency and relieve lending utilities of liability for power outages in their own areas.	(U.S. Congress, Office of Technology Assessment, "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage," 1990).
Convene a panel with representatives from insurance, information technology, and government sectors to examine and propose a plan for government underwritten insurance for information driven losses. Long term goal is to start up this area of insurance and to provide economic motivation for enhancing protection against cyber attacks.	(Copeland, Guy; "Information Assurance Insurance," February 1997).
Quality of Service agreements, agreements between infrastructure service providers or state-federal regulation should be used to encourage reallocation of system load.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).
Government should act to require minimum levels of coverage (as was done with auto insurance) for high risk pools while being careful to maintain the financial health of insurers.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

## XIII. SOLUTIONS RELATING TO ADMINISTRATIVE AND REGULATORY REQUIREMENTS FOR THE PRIVATE SECTOR

Solutions under this category will generally suggest appropriate requirements and vehicles for encouraging or requiring the private sector to act for greater infrastructure assurance. Included within this category will be solutions that suggest whether industry-wide administrative and regulatory requirements, such as mandatory reporting of significant intrusion incidents, would be necessary to maintain an effective indications and warnings system, or whether expanded voluntary compliance, or a system of incentive-based compliance, would provide adequate information when taken in conjunction with information that would be reported by government entities.

### External Considerations

Encourage private industry and the private sector to report intrusions into private information systems through anonymous clearinghouses and similar methods.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Establish independent system operators for the power grid, with access to utility sensitive network information to maintain reliability.	(Coy, Peter; "Who's Watching the Power Grid," Business Week, 1996).
Make investments in improving the technology of firewalls, testers and evaluation tools. Use simulation and training systems for operators which cover a wide range of natural outages as well as malicious attacks.	(DARPA, "Electronic Power Distribution Case Study, Defensive Information Warfare Study," 1995).
Ensure that utilities establish contact with the FBI and coordinate utility emergency plans.	(U.S. Congress, Office of Technology Assessment, "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage," 1990).

Strengthen end system robustness in the financial services industry with multi-function smart cards with cryptographic services, selective cryptographic functions, real-time fault tolerant operating systems, monitor for “anticipatory” system behavior, and use computational service “user agreements.”	(DARPA, Defensive Information Warfare Summer Study Final Report, 1995).
Strengthen network robustness in the financial services industry by using high bandwidth circuits, use authenticated, encrypted virtual circuits, pursue development of bandwidth reservation, use network “user agreements,” employ selective partitioning and routing, and employ a realm-based certification authority structure.	(DARPA, Defensive Information Warfare Summer Study Final Report, 1995).
Manufacturers must ensure that the security capabilities of their goods and services adequately reflect the needs of the market place. Service providers must ensure reliability and assurance of their network services.	(NSTAC, “An Assessment of the Risk to the Security of the Public Network,” 1995).
Users must subscribe to and pay for appropriate levels of privacy and security.	(NSTAC, “An Assessment of the Risk to the Security of the Public Network,” 1995).
Congress promote the convergence of government and private sector interest in cryptography through hearings, evaluation of the Administration’s market study, and encouraging timely, open, and productive dialog.	(U.S. Congress, Office of Technology Assessment, “Issue Update on Information Security and Privacy in Network Environments,” 1995).
Encryption and authentication should be applied to all communications sessions.	(DARPA, “Electronic Distribution Case Study, Defense Information Warfare Study,” 1995).
Encourage Internet Service providers to develop security incident response teams and other security improvement services for their customers.	(CERT Coordination Center, Report to PCCIP, January 1997).
Government should facilitate the development and use of security mechanisms for information in cyberspace that do not undermine commerce or intrude on basic freedoms.	(CERT Coordination Center, Report to PCCIP, January 1997).
Develop, implement, and follow internal reporting procedures within companies that are infrastructure operators.	(OSTP, “Cybernation,” Draft of January 17, 1997).
Develop means for private sector companies with a stake in infrastructure operations to share (within legal limits) information on vulnerabilities, incident data, technical solutions, and best practices, that will adequately protect proprietary or business-sensitive information. Use Network Security Information Exchange (NSIE), NSTAC, within telecommunications industry as a model.	(OSTP, “Cybernation,” Draft of January 17, 1997).

<p>Financial Institutions should implement a robust computer and information security program to include:</p> <ul style="list-style-type: none"> <li>• vulnerability and risk assessment analysis</li> <li>• separation of duties among software development, test and installation personnel</li> <li>• stringent access controls to software and equipment</li> <li>• audit trails</li> <li>• written policies</li> <li>• written contingency plans</li> <li>• CERT capabilities</li> <li>• robust training programs</li> <li>• full-time security positions.</li> </ul>	<p>(Nickson, Mark; “Vulnerability of US Financial Markets to an Information Warfare Attack,” Draft of March 1997).</p>
<p>“The Internet must build in its own protection mechanisms to ensure its survivability.”</p>	<p>(Hughes Electronics Corporation, Report to PCCIP, March 1997).</p>
<p>“All telecommunications providers should initiate efforts to offer Quality of Service (QOS) commitments, as a contractual guarantee.”</p>	<p>(Hughes Electronics Corporation, Report to PCCIP, March 1997).</p>
<p>Telecommunications providers should take measures to contain damage to the local level, making sure architectures are not susceptible to the domino effect.</p>	<p>(Hughes Electronics Corporation, Report to PCCIP, March 1997).</p>
<p>Create a “national incentive program to encourage geographic diversity of network routes,” and robustness.</p>	<p>(Hughes Electronics Corporation, Report to PCCIP, March 1997).</p>
<p>Increase network survivability by:</p> <ul style="list-style-type: none"> <li>• creating a rich path fabric with automatic alternate routing</li> <li>• using geographic dispersal and redundant deployment of critical network facilities</li> <li>• using physical hardening of and water protection for critical network facilities</li> <li>• using distributed control</li> <li>• creating redundant databases with automatic switchover</li> <li>• developing well-designed interconnection standards for use by multiple interfacing</li> <li>• rigorous interoperability testing prior to deployment of service.</li> </ul>	<p>(IDC/LINK, “The U.S. Electronic Distribution Infrastructure: Size, Ownership, Geography, and Vulnerabilities,” March 1997).</p>

<p>Satellite, cable, PCS, and wireless telephone network providers should address the network reliability risk by putting in place the following:</p> <ul style="list-style-type: none"> <li>• firewalls</li> <li>• safeguards to prevent the exportation of problems to other networks</li> <li>• diversity/redundancy to avoid failures in interconnections to the PSTN/cellular/PCS/cable telephone networks</li> <li>• practices to reduce likelihood of AIN related failures</li> <li>• improved standards-based network management systems</li> <li>• cooperation/participation policies in design and development of multi-network interconnection standards</li> <li>• compliance policies and practices for implementing multi-network interconnection interoperability standards and related conformance testing</li> <li>• provisions for hardening and physically dispersing interconnection facilities.</li> </ul>	<p>(IDC/LINK, “The U.S. Electronic Distribution Infrastructure: Size, Ownership, Geography, and Vulnerabilities,” March 1997).</p>
<p>Regulatory agencies should mandate the use of audit systems and establish standards for assuring the integrity of the infrastructure systems under their jurisdiction. Use of public input should be used to balance interests of shareholders, ratepayers, and national leaders.</p>	<p>(Lukasik, Steve; “Public and Private Roles in the Protection of Critical Infrastructure,” March 1997).</p>

## XIV. SOLUTIONS RELATING TO PUBLIC-PRIVATE INVESTMENT INCENTIVES

This category will contain solutions for the implementation of a public-private investment plan (or plans) with incentives to infrastructure owners to cause their voluntary investment in enhanced assurance measures. These measures might include, for example, providing tax credits or changing depreciation schedules for certain percentages of investment in infrastructure assurance. Options for implementation may include the determination of whether a particular protective measure qualifies for receipt of an incentive being tied to the government certifications and standards described previously.

### External Considerations

Make Federal security products and techniques available for use in the NII.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996.)
Promote private sector development of high quality security products and services.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996.)
Consider incentives for industry to develop appropriate security features.	(NSTAC Information Assurance Task Force, "Electric Power Information Assurance Risk Assessment," 1996).
Draw on expertise of insurance industry to develop models and guidelines to better balance the risk equations for infrastructure systems by reflecting the differences in information protection practices.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Encourage academic research into the economic value of information assurance and security to business, by focusing on identifying the value, attributes of information, and models to manipulate information value attributes.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Use incentives, such as tax credits, and government indemnification to improve private sector communication with government.	(SPB Briefing to the Commission, September 23, 1996).

## **XV. SOLUTIONS RELATING TO THE DEVELOPMENT OF NEW RISK MANAGEMENT MODELS**

### **External Considerations**

---

Emphasize individual, commercial, and economic needs in public policy, as well as government and military needs.

(CERT Coordination Center, Report to PCCIP, January 1997).

## XVI. SOLUTIONS RELATING TO PUBLIC AWARENESS AND EDUCATION

Awareness and education solutions might address not only the need for greater awareness of infrastructure vulnerabilities, but also the specific content of such education, the proper entity to conduct such efforts, as well as suggesting proper audiences and methodologies. The effectiveness of advocating or sponsoring a public awareness campaign aimed at increasing awareness of effective assurance practices should be considered. It has been suggested that a more limited, targeted awareness campaign directed at corporate security officers and personnel might be more appropriate to the subject matter at hand.

### External Considerations

Stimulate dialogue and awareness of security risks, needs, and solutions.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996.)
Create an international computer crime bureau to provide education and awareness to foreign law enforcement agencies in order to promote the creation of dedicated computer crime units as well as uniform investigative and computer forensic practices.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Assign an appropriate agency to develop and conduct an awareness program to increase awareness of threats, vulnerabilities and solutions within the electric power industry.	(NSTAC Information Assurance Task Force, "Electric Power Information Assurance Risk Assessment," 1996).
Conduct an awareness campaign to ensure senior-level government and industry representatives are aware of the vulnerabilities and appreciate the implications of Information Warfare. Consider large scale demonstrations, simulations, and experiments, as well as expanding outreach to the public, industry, Commanders-in-Chief (CINCs), services and Agencies.	(Defense Science Board Task Force on IW-D, 1996).
Charter an awareness plan to be promoted by the White House to stimulate increased awareness re-enforcing industry, academic, and government sector efforts. The plan should stress the interests of individual computer users and organizations.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).

Create consumer protection scheme to alert consumers to security risks and protection controls available in computer and network products and services.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Promote academic degree programs in information assurance.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
The Federal government should promote awareness among the private sector of potential vulnerabilities and costs to them of such incidents, as well as the advantage of taking precautions.	(Volpe Center, "Emerging Areas in Transportation Information Infrastructure Security," 1996).
Establish a mechanism for sanitizing and disseminating data on security problems, data that help the network community understand the scope and cost of the overall problem.	(CERT Coordination Center, Report to PCCIP, January 1997).
Government should support the development of educational material and programs about cyberspace for all users, both adults and children.	(CERT Coordination Center, Report to PCCIP, January 1997).
Government should work with industry to create quality user training and comprehensive independent accreditation services.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).
Regulatory proceeding can be used to raise public awareness of infrastructure security threats and requirements through notice of inquiry, notice of proposed rulemaking, or industry advisory panels. Executive branch commissions, task forces and advisory committees or Congressional hearings can serve a similar function.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).
Federal government should use its role as national collector and distributor of national statistics to raise awareness of losses from infrastructure attacks.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

## Federal Role (DoD)

---

### External Considerations

---

Design a curriculum for the study of cyber security including system design, detection of intrusion, intrusion response, firewall design and implementation, and so on. Curriculum could form a new category of engineering in the military academics of an Associates Degree from the Industrial College of the Armed Forces.	(Commissioner Keyes memo, November 6, 1996).
Stress need for proper security training for system administrators, network managers, and chief information officers with long-term goal of promoting undergraduate and master's level training in network and information security.	(CERT Coordination Center, Report to PCCIP, January 1997).

## Private Role

---

### External Considerations

---

Academe should encourage training in the areas of advanced technology and science, including emphasis on primary and secondary school curricula.	(Center for Strategic and International Studies, "R&D for National Strength," 1982).
--	--

## Curriculum (Ethics)

---

### External Considerations

---

Provide early training in security practices and ethics.	(National Research Council, "Computers at Risk," 1991).
Create a grammar school and adult education curricula or class modules to acquaint children and adults (especially parents) with proper ethics and protection pitfalls for interaction in Cyberspace (e.g. property rights, abuse of resources, credit cards, and access codes).	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Government should support programs that provide early training in security practices and appropriate use that is integrated into general education about computing.	(CERT Coordination Center, Report to PCCIP, January 1997).

## XVII. SOLUTIONS RELATING TO PROFESSIONAL TRAINING

This category is devoted to solutions pertaining to enhancing training and professional licensing or certifications for those who work most closely with critical infrastructures.

### External Considerations

Government should support programs that provide early training in security practices and appropriate use that is integrated into general education about computing.	(CERT Coordination Center, Report to PCCIP, January 1997).
Design a curriculum for the study of cyber security including system design, detection of intrusion, intrusion response, firewall design and implementation, and so on. Curriculum could form a new category of engineering in the military academics of an Associates Degree from the Industrial College of the Armed Forces.	(Commissioner Keyes memo, November 6, 1996).
Stress need for proper security training for system administrators, network managers, and chief information officers with long-term goal of promoting undergraduate and master's level training in network and information security.	(CERT Coordination Center, Report to PCCIP, January 1997).
Create a Government Computer Security Specialist and Computer Systems Administrator Career Fields with potential for career progression and incorporate specialized computer security training.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Create a Government Computer Crime Investigators Career Field that includes potential for career progression and specialized computer crime training.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Develop measures to increase the reliability of network operators.	(OSTP, "Cybernation," Draft of January 17, 1997).
Separate the duties of development, test, and installation personnel to minimize success of disgruntled employees and potential effects of innocent errors.	(Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997).

Computer system and software professionals should be encouraged to perform in ways similar to those in the engineering fields through substantial enforcement of licensing, accreditation, responsibility, ethical behavior, legal liability, and incentives for risk management.	(Neumann, Peter; “Security Risks in the Emerging Infrastructure,” Senate Testimony June 1996).
Government should provide long-term support to existing centers of excellence in information and network security to stabilize their funding and ensure their continued existence.	(Spafford, Eugene; COAST/Purdue Univ.; Information Security Education).
Private industry should become more involved with network and information security education and research through funding, personnel and sharing of expertise.	(Spafford, Eugene; COAST/Purdue Univ.; Information Security Education).
Establish programs of scholarships or forgivable loans to students majoring in information security at the graduate level. Make these programs also available to retain appropriately personnel already in the computing profession.	(Spafford, Eugene; COAST/Purdue Univ.; Information Security Education).

## XVIII. SOLUTIONS RELATING TO ENHANCING INTERNATIONAL COOPERATION AND PARTICIPATION IN ASSURANCE PRACTICES

### External Considerations

The Federal Government should promote international cooperation for the protection of the National Information Infrastructure.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996).
Create an international computer crime bureau to provide education and awareness to foreign law enforcement agencies in order to promote the creation of dedicated computer crime units as well as uniform investigative and computer forensic practices.	(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).
Industry should take the lead within existing international industry standards groups to establish international recognition and adaptation of effective security technical and management standards.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Make national policy and operations decisions with the awareness that cyber security issues are international in scope and require international cooperation.	(CERT Coordination Center, Report to PCCIP, January 1997).
Federal government has an obligation to work with other countries to develop compatible cyberspace legal structures and to foster worldwide cooperation among law enforcement agencies.	(OSTP, "Cybernation," Draft of January 17, 1997).
National Security and law enforcement branches of the federal government should facilitate cooperation in the international arena to identify infrastructure threats.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).
Federal government should attempt to further international cooperation in the identification of infrastructure threats by reviewing laws and considering use of formal defense alliance model, such as NATO.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

<p>Government should work toward engineering of international interfaces between national systems. The International Telecommunications Union could provide a valuable model.</p>	<p>(Lukasik, Steve; “Public and Private Roles in the Protection of Critical Infrastructure,” March 1997).</p>
---	---

## XIX. SOLUTIONS RELATING TO EXPORT AND TRADE POLICY

### External Considerations

Clarify export criteria and set up a forum for arbitration for computer and computer security technology.	(National Research Council, "Computers at Risk," 1991).
Launch a dedicated program to establish bilateral and multilateral agreements to adopt compatible legal standards for the use and protection of information systems and products as well as appropriate international criminal codes and definitions of jurisdiction.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
U.S. Government should encourage the use of strong encryption technologies in the private sector, especially the financial sector.	(Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997).
U.S. Government should eliminate regulatory control of development or use of strong crypto, key escrow and key recovery.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).
U.S. Government must take a strong position relating to the protection of personal and corporate privacy including use of nontrivial individual authentication and encryption.	(Neumann, Peter; "Security Risks in the Emerging Infrastructure," Senate Testimony June 1996).

## XX. SOLUTIONS RELATING TO ENHANCING DETERRENCE

Solutions relating to a statement of Administration or Department of Defense policy delineating the degree of proof required to trigger a presumption that a given deleterious act against a critical infrastructure resulted from the concerted activities of a foreign nation (and are thereby akin to an act of war) belong within this category. This category will also include solutions regarding possible statements of U.S. retaliatory intentions, to serve as an effective deterrent and discourage foreign government sponsorship of threatening activities, and enhanced criminal provisions.

### International (DoD)

#### External Considerations

Establish and advertise national policies for protection of vital infrastructures and promulgate strategies for deterring structured attacks.	(CSIS Information Assurance Working Group, Commisisoner Greene memo dated October 2, 1996).
Establish a theory of deterrence for large scale infrastructure attacks analogous to a theory of nuclear deterrence.	(Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997).

## XXI. SOLUTIONS RELATING TO PERIOD OF TRANSITION TO WAR

### External Considerations

---

Information workers should begin to train as defensive information warriors.	(DISA, "Planning Considerations for Defensive Information Warfare- Information Assurance," 1993).
Readiness exercises and war games for defensive information warfare should begin.	(DISA, "Planning Considerations for Defensive Information Warfare- Information Assurance," 1993).
Using an anonymous response, the U.S. government could strike at information terrorists without large display or legitimizing the terrorists, both of which occur with a physical response.	(Devost, Houghton, & Pollard, "Information Terrorism: Can You Trust Your Toaster?," 1996).

---

**XXII. SOLUTIONS RELATING TO  
GOVERNMENT AND CIVILIAN  
RESPONSIBILITIES IN TIME OF WAR  
(DECLARED WAR)**

---

(none identified)

## XXIII. SOLUTIONS RELATING TO EXISTING LEGISLATION/REGULATIONS

Solutions based on amending existing legislation or regulations generally fit into this category. The solutions in this category are aimed at providing infrastructure assurance through modifications of existing legislation, rather than the creation of wholly new laws.

### External Considerations

The Federal Government must develop laws to enable prosecution of those who attack public networks.	(NSTAC, "An Assessment of the Risk to the Security of the Public Network," 1995).
The Federal Government needs to review criminal law to protect the public interest in the National Information Infrastructure.	(Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996.)
Maintain cautious interpretation of the Attorney General's guidelines for online investigations.	(German, Jerry; Testimony on the right to free speech, free association, and privacy on the Internet in the aftermath of Oklahoma City, Senate Subcommittee on Terrorism, Technology, and Government Information, 1995).
Redefine the federal role and responsibilities for assuring the safety of intrastate pipelines, including the hazardous liquids pipelines.	(Comptroller General, "Need to Assess Federal Role in Regulating and Enforcing Pipeline Safety," 1984).
Determine whether there are sufficient hazards involving personal injury or environmental damage to warrant regulation of certain gas and liquid pipeline facilities or commodities not presently covered by federal regulations.	(Comptroller General, "Need to Assess Federal Role in Regulating and Enforcing Pipeline Safety," 1984).

Consider legislation to give the Department of Energy clear authority to make on-site visits to pipeline facilities necessary for identifying and analyzing critical pipelines and related facilities; to develop minimum physical security standards and establish penalties for non-compliance and administrative procedures for appeal; to conduct periodic inspections for determining compliance and for reassessing physical security requirements.	(Comptroller General Report to Congress, 1979).
Create mandatory reporting requirements to support a National Coordinating and Response Center and national deterrence policy for information assurance.	(CSIS Information Assurance Working Group, Commissioner Greene memo dated October 2, 1996).
Create “technology-smart” legislation for cyber-related crimes.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).
Allow users to make copies of copyrighted information and licensed software to protect against loss.	(Hughes Electronics Corporation, Report to PCCIP, March 1997).

# XXIV. SOLUTIONS RELATING TO SHORT-TERM ASSURANCE MEASURES (LOW-HANGING FRUIT)

The solutions in this category have been grouped together because they represent small steps that the Federal government could take, independent of larger endeavors, to shore up the nation’s critical infrastructures. Though these are small steps, they represent important first steps for jump-starting infrastructure assurance efforts.

**External Considerations**

<p>Actions suggested include:</p> <ul style="list-style-type: none"> <li>• develop security policies</li> <li>• form computer emergency response teams</li> <li>• use sound methodology and modern technology to develop high quality software</li> <li>• security standards and participate actively in their design</li> <li>• use technical aids to foster secure operations.</li> </ul>	<p>(National Research Council, “Computers at Risk,” 1991).</p>
<p>Adapt current oversight processes to meet the challenges of the NII.</p>	<p>(Information Infrastructure Task Force Security Issues Forum, “NII Security: The Federal Role,” 1996.)</p>
<p>Create Government Computer Security Specialist and Computer Systems Administrator Career Fields with potential for career progression and incorporate specialized computer security training.</p>	<p>(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).</p>
<p>Create a Government Computer Crime Investigators Career Field that includes potential for career progression and specialized computer crime training.</p>	<p>(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).</p>
<p>Make logon warning banners mandatory for all government and government interest systems.</p>	<p>(U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996).</p>

<p>DoD intelligence agencies should routinely monitor Internet traffic (that is readily accessible to the general public) related to their responsibilities.</p>	<p>(Swett, Charles, OSD; “Strategic Assessment: The Internet,” 1995).</p>
<p>Raise the bar with high payoff, low-cost items including training and awareness programs; improving the security of unclassified computers by eliminating fixed passwords, improving identification and authentication; and promoting use of government approved commercial security technologies.</p>	<p>(Defense Science Board Task Force on IW-D, 1996).</p>
<p>DoD should design a curriculum for the study of cyber security including system design, detection of intrusion, intrusion response, firewall design and implementation, and so on. Curriculum could form a new category of engineering in the military academies of an Associates Degree from the Industrial College of the Armed Forces.</p>	<p>(Commissioner Keyes memo, November 6, 1996).</p>

---

# BIBLIOGRAPHY

---

- ATIS, Network Reliability Steering Committee, "Analysis of Power Related Network Outages," 1996
- Center for Strategic and International Studies, "R&D for National Strength," 1982
- CERT Coordination Center, Report to PCCIP, January 1997
- Comptroller General Report to Congress, 1979
- Comptroller General, "Need to Assess Federal Role in Regulating and Enforcing Pipeline Safety," 1984
- Copeland, Guy; "Information Assurance Insurance," February 1997
- Coy, Peter; "Who's Watching the Power Grid" in Business Week, 1996
- CSIS Information Assurance Working Group, Greene memo dated October 2, 1996
- CSIS, "America's Hidden Vulnerabilities: Crisis Management in a Society of Networks," 1984
- DARPA, "Electronic Power Distribution Case Study, Defensive Information Warfare Study," 1995
- DARPA, Defensive Information Warfare Summer Study Final Report, 1995
- Defense Science Board Task Force on Information Warfare-Defense, November 1996
- Devost, Houghton, & Pollard, "Information Terrorism: Can You Trust Your Toaster?," 1996
- DISA, "Planning Considerations for Defensive Information Warfare- Information Assurance," 1993
- German, Jerry; Testimony on the right to free speech, free association, and privacy on the Internet in the aftermath of Oklahoma City, Subcommittee on Terrorism, Technology, and Government Information, 1995
- Hughes Electronics Corporation, Report to PCCIP, March 1997
- IDC/LINK, "The U.S. Electronic Distribution Infrastructure: Size, Ownership, Geography, and Vulnerabilities," March 1997
- Information Infrastructure Task Force Security Issues Forum, "NII Security: The Federal Role," 1996
- Information Infrastructure Task Force, "NII Risk Assessment: A Nation's Information at Risk," 1996
- K. J. Schrader, "The Army's Role in Domestic Disaster Support: An Assessment of Policy Choices," 1993
- Keyes memo, December 16, 1996
- Keyes memo, November 6, 1996
- Keyes, David; "Stove-Pipe City: It's Not a New Computer Game, It's Why Infrastructure Assurance Needs Centralized Analysis," October 17, 1996, 15
- Logan, Michael; 5<sup>th</sup> International Conference on Information Warfare, 1996
- Lukasik, Steve; "Public and Private Roles in the Protection of Critical Infrastructure," March 1997
- National Research Council, "Computers at Risk," 1991
- National Research Council, "Growing Vulnerability of the Public Switched Networks," 1989
- Naval Research Advisory Council (NRAC) Study, 1996
- Neumann, Peter; "Security Risks in the Emerging Infrastructure," Senate Testimony June 1996
- Nickson, Mark; "Vulnerability of US Financial Markets to an Information Warfare Attack," Draft of March 1997
- NIST, "Assessing Federal and Commercial Information Security Needs," 1992
- NSR, "Indications and Warnings of Strategic Information Warfare," October 1996
- NSTAC Information Assurance Task Force, "Electric Power Information Assurance Risk Assessment," 1996
- NSTAC, "An Assessment of the Risk to the Security of the Public Network," 1995
- OSTP, "Cybernation," Draft of January 17, 1997
- RAND, "Risks to the U.S. Infrastructure from Cyberspace," 1996
- RAND, "Strategic Information Warfare: A New Face of War," 1996
- Spafford, Eugene; COAST/Purdue Univ.; Information Security Education

SPB Briefing to the Commission, September 23, 1996

Swett, Charles, OSD; "Strategic Assessment: The Internet," 1995

U.S. Congress, "Water Quality: A Catalog of Related Federal Programs

U.S. Congress, Office of Technology Assessment, "Issue Update on Information Security and Privacy in Network Environments," 1995

U.S. Congress, Office of Technology Assessment, "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage," 1990

U.S. Security Policy Board, "White Paper on Information Infrastructure Assurance Infrastructure Assurance," 1996

U.S. Senate Permanent Subcommittee on Investigations, Staff Statement: Hearings on Security in Cyberspace, 1996

U.S. Senate Subcommittee on Governmental Affairs, "Draft Committee Report on Network Vulnerabilities to Terrorist Attack, 1989

Volpe Center, "Emerging Areas in Transportation Information Infrastructure Security," 1996

---

---

# **APPENDIX A**

---

---

**U.S. INFRASTRUCTURE ASSURANCE  
Prosperity Game and Planning Event  
March 23-25, 1997  
Chantilly, Virginia**

**SOLUTIONS CATALOG**

# SOLUTIONS CATALOG

## Introduction

The Solutions Catalog consists of 22 broad categories, each comprised of a number of options. Categories and options are presented as “starters” to focus interaction and speed play. They are not intended to discourage players from devising novel solutions, or from modifying those presented. A number of the categories and options are derived from specific observations, proposals and recommendations of prior bodies that have addressed infrastructure assurance issues. Some of the categories and options are included because they reflect solutions invoked during play of the predecessor Prosperity Game™ and Planning Event. Still others appear in the catalog to stir provocative discussion. Players should not take the inclusion (or omission) of any particular category or option to reflect the views or preferences of the sponsors or process managers of this event.

To promote ease of use (and encourage at least a little pre-preparation), the catalog is organized into a workbook format. You are encouraged to review and consider the solution categories (summarized, for convenience, in the table of contents on the following page) prior to the start of the game. You may wish to register your rough sense of preference for a particular solution category in the large check-boxes provided. (Preferences may change through play, so use a pencil!) Players may also wish to register their pre-game preferences for some of the more specific options that are presented within a particular solution category. Smaller check-boxes have been provided for this purpose.

**Note: Although some categories contain options that appear to be mutually exclusive, other categories allow or even encourage the selection of multiple options.**

Please feel free to use these workbooks to capture notes to aid in play of the game. The books will *not* be collected, reviewed, or evaluated by the game staff. However, you will be asked to identify your top six solution category preferences at dinner on the first evening of the event.

**Table of Solution Categories**

	<b>Vigilance</b>
<b>I.</b>	Increase public awareness and education
<b>II.</b>	Enrich training programs for cyber-security professionals, consider licensing or certification
<b>III.</b>	Mandate administrative and regulatory requirements for government and/or the private sector to promote information system security and early warning of threatening cyber attacks
<b>IV.</b>	Develop coordinated national infrastructure assurance policies between government and the private sector
<b>V.</b>	Encourage coordination of national infrastructure assurance policies within the government
<b>VI.</b>	Support creation of a permanent infrastructure protection capability
<b>VII.</b>	Encourage reconsideration of existing Federal department and agency jurisdiction and authority
<b>VIII.</b>	Enhance protection, mitigation, recovery, and emergency response capabilities through development and refinement of coordinated emergency response plans
<b>IX.</b>	Enhance deterrence domestically and internationally
	<b>Network Management</b>
<b>X.</b>	Develop security <i>standards</i> for software, hardware, and network design
<b>XI.</b>	Develop security <i>certifications</i> for software, hardware, and network design
<b>XII.</b>	Promote international cooperation and participation in assurance practices
<b>XIII.</b>	Improve the Federal government’s “model” performance ability (i.e., its ability to influence private-sector action through unilateral efforts at standardization and improved procurement practices)
<b>XIV.</b>	Support creation of a centralized data collection and analysis capability to further development of an effective indications and warnings system
<b>XV.</b>	Accelerate reform of the liability climate
<b>XVI.</b>	Support adoption of public-private investment plans and incentives
<b>XVII.</b>	Encourage government efforts to identify, create, and maintain a “minimal essential infrastructure”
	<b>Technology</b>
	Advance specific technology needs and requirements (cyber)
<b>XIX.</b>	Advance specific technology needs and requirements (physical)
<b>XX.</b>	Promote public-private and government-assisted research and development of specific technology needs and requirements
<b>XXI.</b>	Support mandated adoption of specific technology needs and requirements
<b>XXII.</b>	Develop new risk management tools, models, and techniques
<b>XXIII.</b>	Write in Other Solution Categories: _____

# Solution Categories and Supporting Options

## Vigilance

- I. Increase public awareness and education**
  - A. Support additional government funding of Federal, state, and local educational programs to expand public awareness of physical and cyber-security issues.
  - B. Support creation of grammar, middle, high school, and adult education curricula to acquaint children and adults with rules and norms for interactions in cyber space (including ethics, property rights, abuses of resources, theft of services, etc.).
  - C. Charge government entities such as the National Science Foundation to develop educational programs in resilient system design and practices for implementation at undergraduate and graduate levels.
  - D. Support a tax credit for private insurance companies to conduct educational programs to include infrastructure assurance measures in business practices and reduce the likelihood of debilitating loss through insurance claims.
  - E. Organize resources to participate in joint government-private sector programs to increase threat and vulnerability awareness of senior-level government and industry policy makers, to include, for example, demonstrations and simulations of key vulnerabilities.
  - F. Same as E., above, but targeted at middle managers.
  - G. Other (describe) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



**II. Enrich training programs for cyber-security professionals, consider licensing or certification**

- A. Support development and adoption of degree programs in cyber security (including system design, intrusion detection and response, firewall design, etc.) for inclusion in military college curricula.
- B. Support addition of security training modules to existing computer science curricula.
- C. Support development and operation of a government licensing system for certain categories of computer professionals (e.g., “driver’s licenses” for particular programmer and system administrator positions) with criteria for technical and ethical excellence. Licensing would be required for those holding certain sensitive positions with government and infrastructure service providers.
- D. Support development and operation of a private sector certification body for certain categories of computer professionals. Certification, though not required, would likely carry insurance and liability-related benefits for private-sector participants.
- E. Support and fund the development of a government-private-sector, performance-based certification standard for computer professionals, to be used by government and the private sector to guide personnel decisions.
- F. Other (describe) \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_



**III. Mandate administrative and regulatory requirements for government and/or the private sector to promote information system security and early warning of threatening cyber attacks**

A. Regulations are to be binding on (check all that apply):

- 1. the Federal government, including military installations
- 2. state and local governments
- 3. schools and universities (as prerequisite to receiving Federal funds)
- 4. all infrastructure service providers
- 5. all businesses having more than 50 employees with remote access capabilities
- 6. Other(describe) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

B. Regulations are to provide for (check all that apply):

- 1. mandatory reporting of significant infrastructure service outages
- 2. mandatory reporting of significant cyber-intrusion incidents
- 3. mandatory use of authentication controls such as one-time password generators
- 4. mandatory use of strong access controls (e.g., firewalls, strong authentication) to protect Supervisory Control and Data Acquisition (SCADA) information
- 5. mandatory encryption of SCADA information
- 6. mandatory reserve capacities and redundancy margins
- 7. Other(describe) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**IV. Develop coordinated national infrastructure assurance policies between government and the private sector**

- A. Support tasking of an existing Federal cabinet-level agency to assume policy-level infrastructure assurance responsibilities, including coordinating public-private infrastructure assurance activities and devising appropriate funding vehicles for these activities.
- B. Advocate creation of a new cabinet-level agency to accomplish the above (e.g., an “Infrastructure Protection Agency”).
- C. Establish an information security/infrastructure assurance focus within an existing White House policy entity, such as the National Security Council or National Economic Council, to assume policy-level infrastructure assurance responsibilities, as in IV.A. above.
- D. Support legislation or other legal measures to create a new Federal policy entity, within the White House, to assume infrastructure assurance responsibilities as in IV.A. above.
- E. Support legislation or other legal measures creating a governmental public policy entity, such as the Federal Reserve Board, to assume policy-level infrastructure assurance responsibilities as in IV.A. above. (The board would be comprised of Presidential appointees, confirmed by the Senate, who are appointed to terms as full-time government employees).
- F. Support legislation or other legal measures creating individual infrastructure advisory committees, based on a National Communications System - National Security Telecommunications Advisory Committee (NCS-NSTAC) model, to assume policy-level responsibilities as in IV.A. above and coordinate pre-competitive approaches to infrastructure assurance. (NSTAC is a Presidential Advisory Committee of 23 corporations representing the telecommunications infrastructure. The NCS represents the Federal agencies responsible for telecommunications in the U.S. and operates in close coordination with the NSTAC).
- G. Accomplish policy level input to the government through an exclusively private-sector consortium of corporate officers assembled according to their ability to represent diverse infrastructure interests.
- H. Other (describe)  
\_\_\_\_\_  
\_\_\_\_\_

**V. Encourage coordination of national infrastructure assurance policies within the government**

- A. Support tasking of an existing Federal cabinet-level agency to coordinate infrastructure assurance efforts of the Federal government.
- B. Establish an information security/infrastructure assurance focus within an existing White House policy entity, such as the National Security Council or National Economic Council, to assume policy-level infrastructure assurance responsibilities, to include organization and funding of public-private assurance efforts.
- C. Support appointment of a full-time government board, made up of qualified Federal-government employees, to facilitate implementation of national infrastructure assurance policies throughout government, and to coordinate government activities to improve efficiency and avoid redundancy.
- D. Support appointment of a full-time, public-private-sector board to facilitate implementation of national infrastructure assurance policies throughout the government, with enhanced ability to track developments in the private sector.
- E. Fund and support a full-time private-sector entity, to work in parallel with government efforts and consult with the government as to how best to facilitate implementation of national infrastructure assurance policies.
- F. Other (describe) \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**VI. Support creation of a permanent infrastructure protection capability**

- A. Support the development, within the Federal government, for the exclusive benefit of Federal, state, and local governments, of a capability to provide or facilitate provision of expert guidance to halt or confine attack and restore service.
- B. Support the development, within the Federal government, for the benefit of governments *and* the private sector, of a capability to provide or facilitate provision of expert guidance to halt or confine attack and restore service.
- C. Support the development, within the Federal government, of a capability to receive specific threat information, and issue threat and warning notices to government and the private sector based on such reports and information collected and analyzed by the mechanism described above.
- D. Support the development, within the academic community and private sector, of a capability to receive specific threat information, and issue threat and warning notices based on such reports (e.g., an expanded Carnegie-Mellon Computer Emergency Response Team (CERT) capability).
- E. Support the development, within the Federal government, of an independent administrative body, such as the National Transportation Safety Board, to hire qualified staff to perform investigations of infrastructure-threatening incidents, then issue recommendations for further action.
- F. Other (describe) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**VII. Encourage reconsideration of existing Federal department and agency jurisdiction and authority**

- A. Ensure appropriate Federal agencies have the authority, mission, and responsibility to assist other Federal agencies in information infrastructure protection efforts, including review of proposed or planned system architectures and sharing of information on countermeasures.
- B. Ensure appropriate Federal agencies have the authority, mission, and responsibility to assist other Federal agencies, state and local governments, and industry, in information infrastructure protection efforts, including review of proposed or planned system architectures and sharing of information on countermeasures.
- C. Expand existing defense community jurisdiction to address threats to the infrastructure (by, for example, providing technical support to law enforcement in criminal investigations and disaster recovery services to the private sector).
- D. Expand existing intelligence community jurisdiction to address threats to the infrastructure (by, for example, allowing limited collections relating to vital infrastructure protection functions, whether such needs arise in the U.S. or abroad).
- E. Expand existing law enforcement community jurisdiction to address threats to the infrastructure (by, for example, expanding its ability to compel assistance from the defense and intelligence communities to fulfill its investigative or protective functions).
- F. Expand jurisdiction of other regulatory and administrative bodies and/or Federal agencies to address threats to the infrastructure.
- G. Other (describe) \_\_\_\_\_

---

---

**VIII. Enhance protection, mitigation, recovery and emergency response capabilities through development and refinement of coordinated emergency response plans**

- A. Task military branches to accept and adopt civil disaster response as a mission for active and reserve forces.
- B. Amend the Federal Response Plan and associated authorities to expressly include ability to address critical cyber-incidents, greater use of mitigation tactics, and funding authority to more effectively coordinate services following an infrastructure attack.
- C. Provide incentives for proactive state-government disaster mitigation efforts (e.g., improved building codes, emergency response, training for disaster response personnel), and other measures to reduce damage from a major, infrastructure threatening occurrence.
- D. Support formation of a public-private “emergency corps” to assist in repair and recovery following infrastructure threatening occurrences.
- E. Other (describe) \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**IX. Enhance deterrence domestically and internationally**

- A. Adopt or amend legislation to more clearly criminalize intentional or willful attacks on, damage to, or destruction of critical infrastructures.
- B. Enhance deterrence domestically through aggressive public awareness campaigns equating damage to government systems with sabotage, and intrusions into private systems with other, analogous crimes.
- C. Encourage the U.S. Government to make known, through “back door” diplomatic channels, its ability to anonymously strike back at information terrorists without the display of force or publicity that would otherwise legitimize the terrorist activity.
- D. Encourage the U.S. Government to make widely known the degree of proof that would be required to trigger a presumption that certain infrastructure failures resulted from concerted activities of a foreign nation, thereby constituting an act of war subject to retaliatory action through cyber means or deployment of conventional forces.
- E. Other (describe) \_\_\_\_\_

---

---

## Network Management

**X. Develop security *standards* for software, hardware and network design**

- A. Support efforts by government standard-setting bodies, such as the National Institute of Standards and Technology (NIST), to develop security standards for software, hardware, and network configuration for Federal government systems. (Although not binding on the private sector, compliance with standards would likely carry insurance and liability-related benefits).
- B. Support efforts by an appropriate policy authority (such as described in Category IV., above) to develop security standards for providers of infrastructure services, compliance to be enforced through administrative sanctions.
- C. Support creation of exclusively private-sector bodies to develop appropriate security standards to apply to providers of infrastructure services, compliance to be enforced through administrative sanctions. (This may require that certain legal restrictions be relaxed for this limited purpose).
- D. Support creation of exclusively private-sector bodies to develop appropriate security standards for providers of infrastructure services, compliance with which is voluntary but will likely carry insurance and liability-related benefits.
- E. Other (describe) \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XI. Develop security *certifications* for software, hardware, and network design**

- A. Encourage Federal standard-setting agencies, such as the National Institute of Standards and Technology (NIST), to develop a system of *government* certifications for software, hardware and network configuration. (Although the certifications would not be available to the private sector, compliance with underlying requirements would likely carry insurance and liability-related benefits).
- B. Support tasking of an appropriate policy authority (see Category IV., above) to develop thresholds and procedures for issuance of certifications to qualified government and private-sector applicants (i.e., the rough equivalent of an Underwriter's Laboratory for cyber certifications).
- C. Fund and support existing private-sector standards bodies to develop thresholds and procedures for businesses to receive certifications as above.
- D. Encourage creation and funding of new private-sector standards bodies to develop thresholds and procedures for businesses to receive certifications as above.
- E. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XII. Promote international cooperation and participation in assurance practices**

- A. Support creation of an international computer crime bureau to provide education, awareness, and investigative assistance to foreign law-enforcement agencies.
- B. Encourage Federal standard-setting agencies, such as the National Institute of Standards and Technology (NIST), to participate in the development of voluntary international standards or certifications for software, hardware, network configuration, and trusted network personnel.
- C. Support the tasking of an appropriate policy authority (see Category IV., above) to participate in the development of voluntary international standards or certifications as above.
- D. Support and fund exclusively private-sector bodies to develop voluntary international standards or certifications as above.
- E. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XIII. Improve the Federal government’s “model” performance ability (i.e., its ability to influence private-sector action through unilateral efforts at standardization and improved procurement practices)**

- A. Mandate that all new legislation considered by Congress and all deregulation actions considered by Federal agencies that affect critical infrastructures include an “Infrastructure Assurance Impact Statement” that fully explores expected positive and negative effects of these measures on infrastructure assurance objectives.
- B. Support legislative initiatives that require Federal, state, and local governments to unify and improve government procurement standards and practices to reflect preferences for purchasing and implementing products that promote system security.
- C. Allocate resources to work with Federal, state, and local governments, through a policy authority (such as in Category IV., above) to accomplish as stated in B., above.
- D. Support and fund exclusively-private-sector bodies to recommend to Federal, state, and local governments appropriate procurement standards and practices.
- E. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XIV. Support creation of a centralized data collection and analysis capability to further development of an effective indications and warnings system**

- A. Support legislation requiring the government to share sufficiently reliable threat information with the private sector.
- B. Support tasking of existing government resources within the defense, intelligence, and law-enforcement communities (and state and local governments) to develop centralized data collection and analysis at existing levels of funding, and share threat information with the private sector.
- C. Support measures that dramatically increase funding for the development of government data collection and analysis capabilities with threat information to be shared with the private sector, *without* having to rely on specific threat or vulnerability input from the private sector.
- D. Support measures that increase contributions by the private sector to fund additional government data collection and analysis capabilities, to then share threat information, *and* contribute proprietary threat or vulnerability information under conditions that such information would remain confidential.
- E. Same as above, but only under the condition that specific threat and vulnerability information from the private sector be contributed anonymously.
- F. Designate/create a single, independent, trusted organization to be responsible for collecting, analyzing, and reporting incident data, with no public policy, investigation, or enforcement authority.
- G. Other (describe)\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**XV. Accelerate reform of the liability climate**

- A. Create a new Financial Accounting Standards Board (FASB) standard relating to information security so that companies regulated by the Securities and Exchange Commission (SEC) would be audited against it and, if their efforts are not adequate, will have a contingent liability noted on their financial statements.
- B. Extend the Federal Deposit Insurance Corporation (FDIC) concept to insure against catastrophic infrastructure loss by creating an entity to insure deposits against losses that are not currently insurable, such as losses from electronic commerce and harm from acts of terrorism. Funding would come from a tax on transactions in each respective infrastructure.
- C. Support legislation creating liability for providers of infrastructure services who fail to meet standards of due care--which failure then results in damaging loss of service to customers.
- D. Support legislation capping liability for providers of infrastructure services who meet certain standards or certifications.
- E. Encourage providers of infrastructure services to form coalitions to develop guidelines for reliability, reserve capacity, etc., to inform and influence standards of due care within infrastructures.
- F. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XVI. Support adoption of public-private investment plans and incentives**

- A. Create an organizational entity within the Executive Branch, similar to the “superfund” structure, financed by tax dollars, to assess and ameliorate the most critical vulnerabilities to infrastructure assurance when responsibility for the deficiencies cannot be assigned to a responsible and financially viable legal entity.
- B. Tie receipt of targeted financial incentives to compliance with standards or certifications such as those described in Categories X. and XI., above.
- C. Support permanent (not year-to-year) tax credits for investment in research, development, or deployment of measures specifically devoted to increasing the assurance of the infrastructure.
- D. Support an accelerated depreciation schedule for investments in information-related hardware to coincide with the actual lifetime of the equipment so that companies will be motivated to more aggressively upgrade their level of service with accompanying improvements in security, reliability, and interoperability.
- E. Change Federal income tax rules, which currently treat all funds retained at the end of the tax year as taxable profit, to encourage private insurers to retain adequate funds in reserve for emergencies.
- F. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XVII. Encourage government efforts to identify, create and maintain a “minimal essential infrastructure”**

- A. Support Federal government programs to identify critical nodes within the government, assess their vulnerabilities and interdependencies, and make recommendations to funding authorities for cost-effective protections and improvements.
- B. Support Federal efforts to revitalize critical asset assurance and protection programs to include involvement by Federal, state, and local governments.
- C. Support government efforts to identify a minimal essential information infrastructure for use in restoring services and adapting to wide-scale outages.
- D. Support Federal-government programs to identify elements of public and privately-owned information which collectively comprises “vital national information interests,” including physical infrastructure components, virtual processes, and some forms of information.
- E. Support government efforts to subsidize additional reserve capacities for assets comprising the minimal essential infrastructure.
- F. Work with private sector consortia to develop infrastructure-wide agreements establishing service priorities in the event of major infrastructure outages.
- G. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

# Technology

## XVIII. Advance specific technology needs and requirements (cyber)

- A. Develop robust, survivable system architectures that include advanced firewall technology.
- B. Develop techniques and tools for modeling, monitoring, and managing large-scale distributed/network systems (including practical techniques and tools for system administrators to determine the security condition of their network including the strength of the various security mechanisms and the system's vulnerability to threats).
- C. Develop techniques and tools for auditing, detecting, and responding to intrusions into large-scale distributed/network systems.
- D. Develop techniques and tools for using encryption technologies to address surety and security deficiencies.
- E. Develop administrator-friendly strong access controls (e.g., superior firewalls, stronger authentication, effective intrusion countermeasures, and isolation techniques that do not directly depend on encryption) to protect Supervisory Control and Data Acquisition (SCADA) from cyber attack.
- F. Research and develop truly adaptive software that scans a control system's sensor suites and SCADA programs for evidence of unusual activity and provides warnings and indicators of impending problems from critical nodes, intrusions, unexpected interdependencies, or outdated hardware or software.
- G. Research and develop new breakthrough architectures, comparable to the invention of packet switching in the 1960's, that are self-healing independent of traffic rate to improve robustness and survivability under cyber attack and under abnormal loading.
- H. Develop means for dynamically reallocating communication resources to give priority to critical messages such as emergency preparedness, national security, or system security communications even if the network is overloaded with normal traffic.
- I. Other (describe) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



**XIX. Advance specific technology needs and requirements (physical)**

- A. Develop and deploy a sensor system (such as a UV laser-induced fluorescence system for non-intrusive screening or neutron-induced activation with x-ray emission) that remotely interrogates vehicles for explosives.
- B. Develop cost-effective chemical/biological detectors (including procedural guidelines governing their use) for placement in facilities such as buildings, subways, and other places where large numbers of people congregate.
- C. Other (describe)\_\_\_\_\_

---

---

**XX. Promote public-private and government-assisted research and development of specific technology needs and requirements**

- A. Support tasking existing government resources to coordinate government research and development efforts and expand government R & D on cyber-resilient technologies, such as firewalls, auditing, monitoring, and intrusion detection technologies, and encryption. Expansion of these efforts will occur at the expense of current government R & D priorities.
- B. Support enhanced funding for existing government mechanisms to coordinate and expand government research and development efforts on cyber-resilient technologies, and to procure targeted research and development from the private sector.
- C. Support grants for research and development through Cooperative Research and Development Agreements (CRADAs) specifically targeting infrastructure assurance objectives, and provide Federal agencies, the national labs, and industry consortia with incentives to develop and deploy new technologies.
- D. Create a process whereby the government directly develops technology and transfers it to the private sector through an “Infrastructure Investment Bank” for targeted use in infrastructure strengthening.
- E. Support the creation of a government corporation (such as the U.S. Synthetic Fuels Corporation) to guide sizable government investment in private sector research and development on cyber-resilient technologies.
- F. Support the creation of a joint government-industry research corporation (such as Sematech) to employ government, academia, and private sector experts for limited terms to focus on research and development of cyber-resilient technologies, and to provide support to other emerging centers of excellence.
- G. Support and fund coordinated programs to facilitate technology transfer from government to the private sector with respect to new cyber-resilient technologies.
- H. Support coordinated and focused private-sector research and development efforts through the creation of exclusively private sector alliances and through the suspension of existing impediments to enhanced cooperation.
- I. Other (describe) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**XXI. Support mandated adoption of specific technology needs and requirements**

- A. Support legislation mandating the adoption, when ready for deployment, of selected technology needs and requirements, such as those identified in Categories XVII. and XIX., above, by Federal, state, and local governments.
- B. Support legislation mandating the adoption, when ready for deployment, of the selected technology needs and requirements, such as those identified in Categories XVII. and XIX. above, by Federal, state, and local governments and infrastructure service providers.
- C. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XXII. Develop new risk management tools, models and techniques**

- A. Facilitate inclusion of risk data in ongoing government data collection activities, such as those conducted by the Census Bureau or the National Economic Council.
- B. Establish a separate risk category for information system security for regulators to use in their risk-based oversight of critical infrastructure industries.
- C. To reduce risk of harmful insider threats, develop and deploy new personnel and management approaches that keep employees positively engaged.
- D. Develop practical metrics for determining the security condition of a network, including the strengths of various security mechanisms, current known and potential threats and vulnerabilities, and potential impacts in a graded methodology to assist system administrators.
- E. Develop tools, models, and methods that help system designers make decisions affecting the system-level robustness in their economic selection studies.
- F. Support establishment of a joint government/private sector institute to study and develop new risk management models, and to provide education to senior-level government and industry policy makers.
- G. Same as above, but limited to a private-sector consortium.
- H. Other (describe)\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**XXIII.Other (describe)**

---

---

---

---

---

---

---

---

---

---