US INFRASTRUCTURE ASSURANCE PROSPERITY GAME™ FINAL REPORT

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

This report was prepared for the President's Commission on Critical Infrastructure Protection. The report represents the opinions and conclusions solely of its developer, Sandia National Laboratories with Prosperity Institute. The Commission has not made a judgment on, nor should the publication of this document be taken to represent an endorsement by the Commission for the content of the material contained herein.

Table of Contents

US Infrastructure Assurance Prosperity Games™ Sponsored by:

President's Commission on Critical Infrastructure Protection (PCCIP)

National Communications System (NCS)

Department of Energy (DOE) Nonproliferation & National Security Office (NN-50)

Sandia National Labs Strategic Surety Program Office

This report represents a summary of the results of the US Infrastructure Assurance Prosperity Games™. It is intended to provide information to the deliberations of the President's Commission on Critical Infrastructure Protection (PCCIP). This report does not necessarily represent the positions of, nor speak for, the PCCIP. This report is neither a recommendation nor a roadmap.

Introduction

Sandia National Laboratories, with Prosperity Institute, designed the US Infrastructure Assurance Prosperity Games™ to identify and assess strategy options for increasing the surety and security of the nation's critical infrastructures. This report details the results identified by the participants of the two Prosperity Games™ executed for that purpose.

Prosperity Games™

Prosperity Games™ were developed by combining strategic war gaming with the emerging understanding of how executives in major multi-national corporations exercise discretion and judgment to build the future prosperity of their enterprises. Prosperity Games™ integrate leadership development and strategy development to create an engaging experience of immediate relevance to the participant and his or her organization. The Games model the complex world of value propositions and persuasion: they are not people playing against a computer. The play takes place in an unstructured, open environment with limited, yet pertinent, information.

The Games feature the processes of preparation, planning, follow through and the use of feedback to inform participants about their relative success in achieving the objectives of the game. Players control the content of the games and generate their own options, which are major outcomes of the games. High-level players create new insights and options that illuminate opportunities. Players who engage with others in the game to create consensus and test each other's ideas benefit the most.

Teams are designed to provide the optimum knowledge and judgment necessary to make decisions and diversity to create stimulating and engaging interactions. The degree of teamwork and the types of strategies developed are determined by the team. See Appendix B "Levels of Strategy" of the US Infrastructure Assurance Prosperity Game™ 1 Player's Handbook for a description of the progression of strategy sophistication stimulated by the game dynamics.

An Important Constituency: the Infrastructure Practitioner

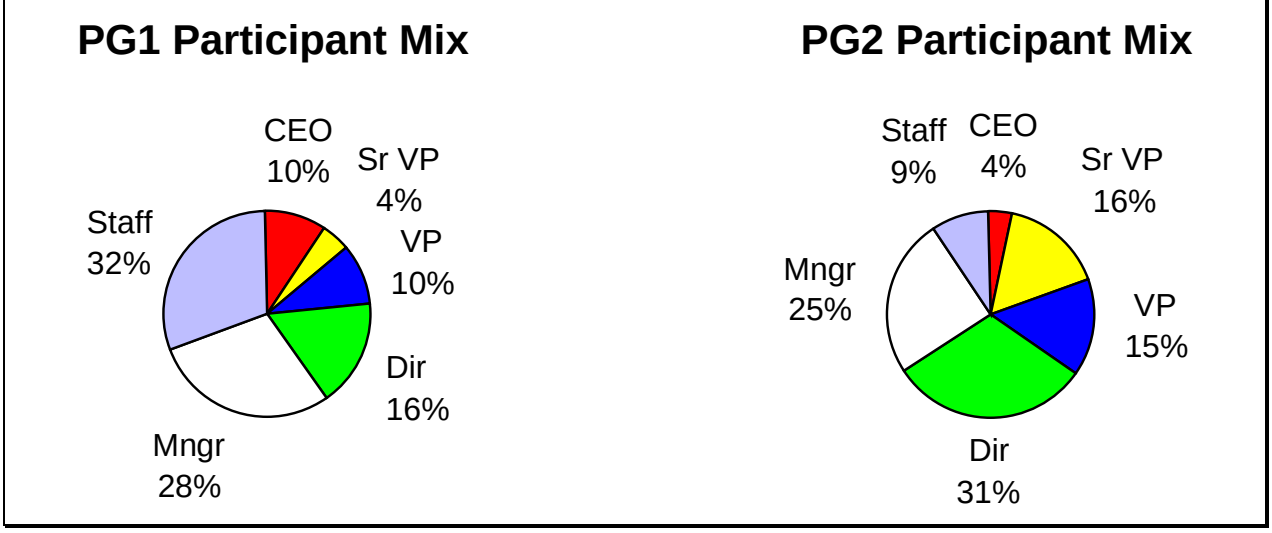
The Prosperity Games™ provided a unique perspective as an input to the deliberations of the President's Commission on Critical Infrastructure Protection (PCCIP). The Prosperity Game™ process was designed to draw on the cumulative experience and judgment of the game participants: stakeholders knowledgeable of their infrastructure and experienced in formulating far-reaching practical policies, practices, and technology options. Sandia canvassed potential participants for the Games and extended invitations to stakeholders representing a broad cross-section of ownership and assurance responsibilities within each infrastructure sector. The PCCIP was instrumental in identifying the potential participants. As a result, the Games extracted the views and assessments of the infrastructure practitioners (i.e., those with ownership and responsibility for the US infrastructure) in addition to the security expert: ***Response from infrastructure practitioners complements other inputs that the PCCIP has obtained from experts within the security communities.***

The Games' participants were not all security experts, but had varying levels of experience and awareness about infrastructure protection. Game 1 was served as a prototype for Game 2 and

focused on responses from the various infrastructure protection operations communities. Sixty percent of the Game 1 participants held staff or first level management responsibilities.

Game 2 emphasized response from those making strategic infrastructure protection decisions. Such response was essential to address the advantages and disadvantages of the 22 solution categories being considered and catalogued by the PCCIP. Sixty six percent of the Game 2 participants held executive level management positions (see Figure 1).

Figure 1. Game participants had varying levels of experience and infrastructure protection responsibilities



Infrastructure stakeholders from industry and government organizations often times represent different needs and interests and maintain different points-of-view on key issues. The Games promoted discussion of those different viewpoints in small groups and synthesized them into a working consensus: one in which all parties could support, even if they were not optimal for a particular interest group.

The Games were intended to have strong participation from both industry and government to provide a reasonably balanced view. Each participant declared their constituency as industry or government during voting sessions. The participation statistics indicated that 42 percent of the players represented private industry and 58 percent represented government organizations for each Game (see Figure 2). About one-third of the Game 1 industry players had specific infrastructure security expertise, primarily in physical protection applications. Nearly half of the Game 2 industry participants had specific infrastructure security expertise, with an emphasis on cyber security expertise.

It should be noted that the views from these practitioners provide important feedback to the PCCIP and other sponsors about the general awareness of the threat and provide a measure of receptivity of the community to proposed solutions for protection of the US infrastructure.

Overall, the results of the Games are representative of the audience that will be highly interested in the Commission's report.

Figure 2. Game participants represented public and private practitioner and security perspectives

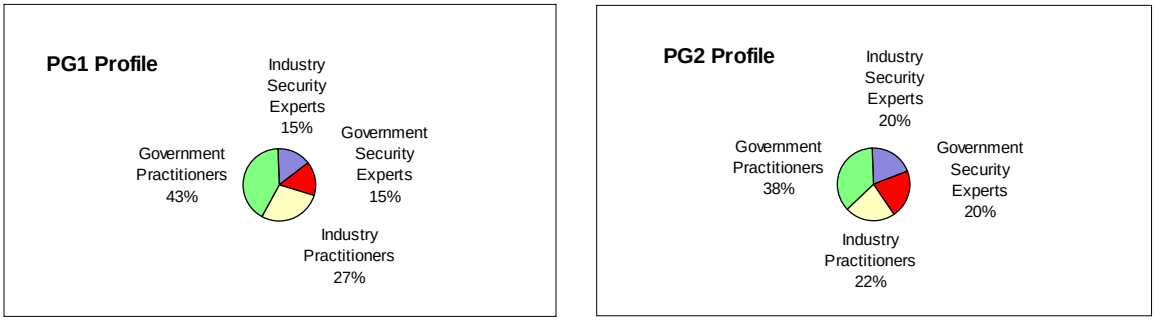
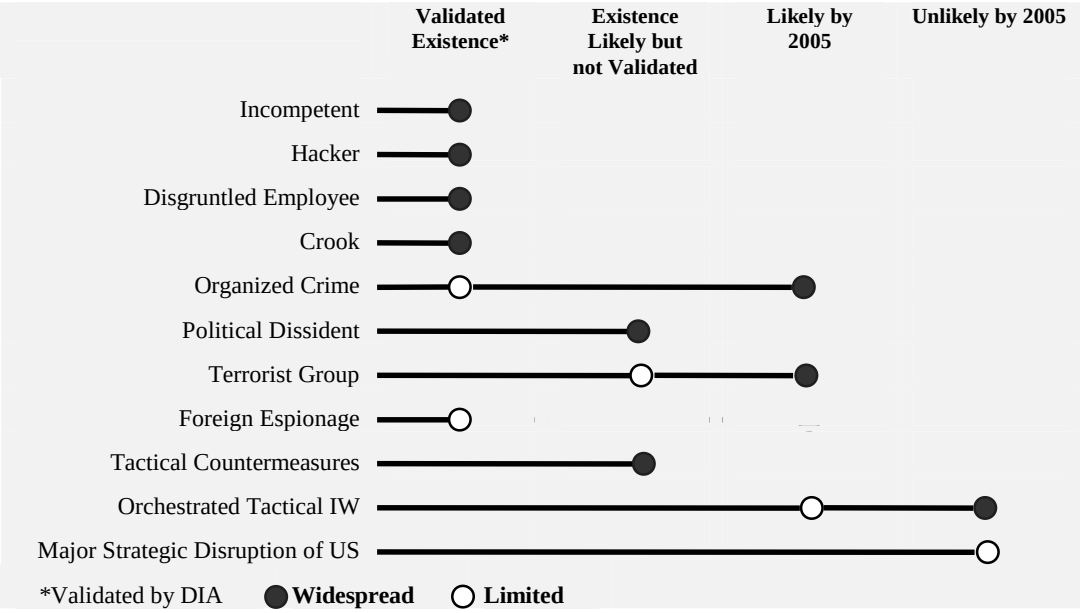


Table 1. Cyber Threat Assessment 1997 - 2005. Source: DSB Task Force Report on Information Warfare - Defense



Context for Prosperity Games™

The scope for the Games addressed the threat and vulnerability circumstances currently faced by the nation's infrastructures and looked 15 years into the future. During this timeframe, the nation is envisioned to become more vulnerable to cyber threats due to its growing dependence on

computers and communications systems to run its critical infrastructures. As an example, the Defense Science Board (DSB) Task Force on Information Warfare--Defense states the threat of information warfare to be significant. Although hackers tend to dominate the news headlines, the DSB Task Force identified that the emerging threat is primarily from structured attacks by organized crime, terrorist groups, and foreign espionage, as summarized in the DSB assessment (see Table 1).

Emerging Threats and Vulnerabilities

The Prosperity Games™ utilized the results from prior studies and experts' response on the threats and vulnerabilities of critical infrastructures and organized them as potential solution options to stimulate the Game participants creativity in addressing challenges for the protection of the nation's infrastructures. By means of the gaming process, the Game 1 participants prioritized a number of potential infrastructure solution categories. The first Game's top solution categories were integrated with solution categories from other PCCIP sources to form the baseline of the Commission's Solution Catalog (see Solution Catalog beginning on page 9 of the Game 2 Player's Handbook). The Solution Catalog consists of 22 solution categories being considered by the Commission from which recommendations will be made to address emerging threats and vulnerabilities. These solution categories were provided as the principal input to the Game 2 participants to assess their feasibility in addressing the emerging threat, the interdependencies among infrastructures due to emerging technologies, as well as their potential as a model for collaboration among organizations to protect infrastructures.

Examples of emerging threats, interdependencies, and collaboration challenges that were considered by the Game participants are as follows:

Emerging threats

- Cyber threats
- Physical threats enhanced by or directed at cyber systems
- Threats arising from increasing complexity of interdependent infrastructures

Technology-based Interdependencies

- Inadequate ability to predict consequences of events in complex system of systems
- Cyber-accessible open sources for Intelligence to plan attacks
- Vulnerabilities from network enabled Supervisory Control And Data Acquisition (SCADA) systems, including greater potential for single point failures
- Industry-standard software replaces proprietary software
- Cyber enabled Just-In-Time system reduces stockpiles to handle contingencies
- Multiple levels of potential vulnerability -- data, network, and underlying infrastructure

Trend Generated Complexity Interdependencies

- Globalization of information access, standards, business, and single source suppliers and foreign ownership of companies providing services in the US Infrastructure
- Deregulation, increasing competition, and decreasing margins
- Electronic Commerce as alternative currency to nation-state currency

Models for Collaboration or Relationship

- Government Department with Government Department
- Government with Industry
- Industry with Industry

US Infrastructure Assurance Prosperity Game™ 1

Game 1 Objectives

The objectives of the first Game included the following:

- Assess the scope and nature of the vulnerabilities of and threats to the nation's infrastructure
- Develop an educated understanding of the driving forces, metrics, consequences, and proactive and reactive options for improving infrastructure assurance
- Develop, test, improve, and prioritize strategies for increasing infrastructure assurance
- Develop strategic roadmaps that define the policy, process, and technology options that need to be pursued
- Develop a strategic consensus amidst many conflicting points of view by exploring relationships and partnerships amongst key stakeholders

Game 1 Teams

Game 1 participants were assigned to teams representing the following infrastructures:

- Electric Power
- Emergency Services
- Finance & Banking
- Insurers
- Oil & Gas
- Telecommunications
- Transportation: Air
- Transportation: Land & Water
- Water

With the exception of the Emergency Services and Insurers Teams, each infrastructure sector was represented by both a Blue Team and a Red Team to execute strategies for the protection of their infrastructure, and to execute attacks to capitalize upon a vulnerability of an infrastructure(s), respectively.

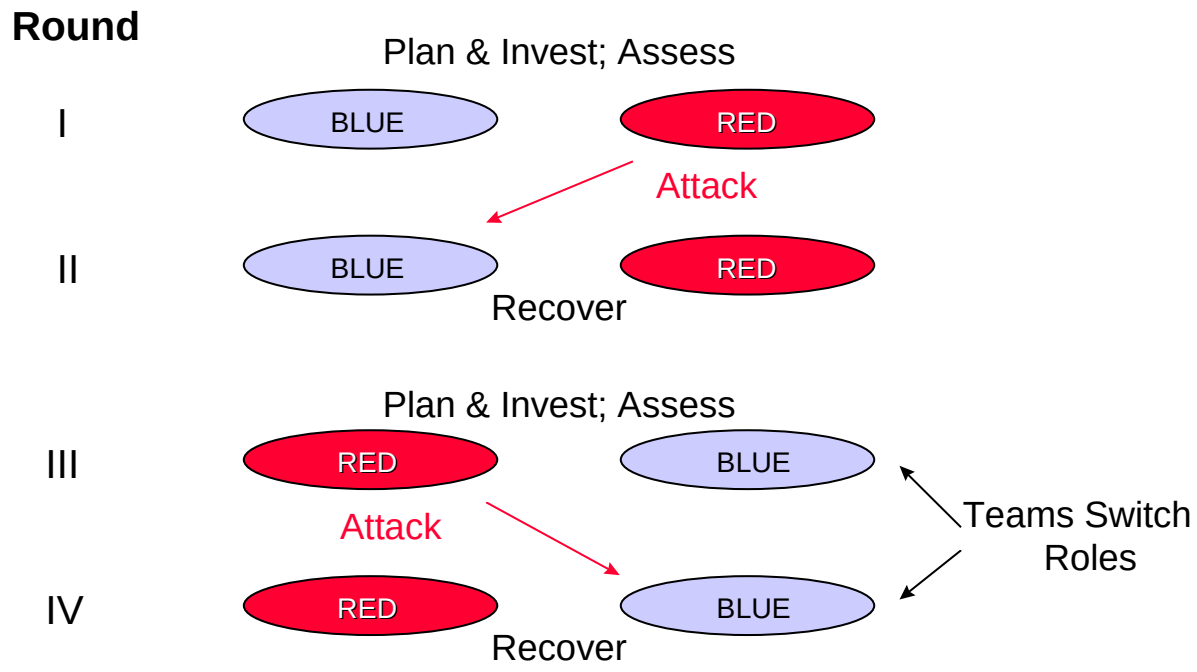
Game 1 Design

The Game 1 process featured four rounds of planning with assessment of a team's strategies. During Round 1, within the budget and resource constraints of each infrastructure, Blue Teams developed strategic plans, based on investments in solution categories, to protect their critical assets against perceived threats and known vulnerabilities. Simultaneously, Red Teams worked within much reduced budget and resource constraints to identify actions for upsetting a Blue

Team or a set of interdependent Blue Teams. During Round 2, each Blue Team worked through a series of steps (if required) to recover from the Red Team upset actions.

Rounds 3 and 4 followed the same processes of Blue Team planning and investment, and Red Team identifying upset actions with the exception that the Blue Team participants in Rounds 1 and 2, now assumed the role of a corresponding Red Team, and Red Team participants in Rounds 1 and 2, took the role of a corresponding Blue Team (See Figure 3).

Figure 3. Game 1 Process

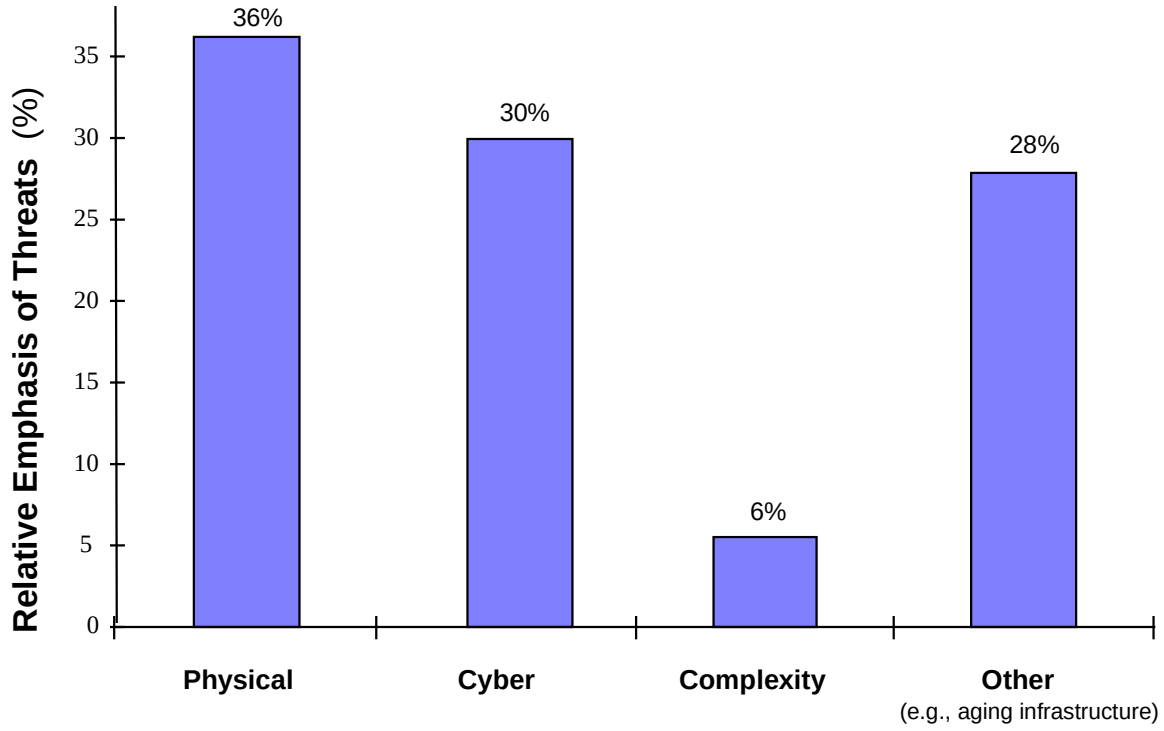


Game 1 Identified Infrastructure Assurance Solution Priorities

The solution categories resulting from the Game 1 Blue Teams' strategic plans provided a basis for determining the relative importance of potential infrastructure assurance solutions.

For example, the relative awareness of the practitioner to the vulnerability of the nation's infrastructures to the physical, cyber, complexity and other threats is shown in Figure 4. The vertical axis represents the percentage of total solutions identified by Blue Team strategic plans. The horizontal axis represents the four broad areas in which strategic plan solutions were developed to address types of threats and vulnerabilities: physical, cyber, complexity (e.g., interdependencies between infrastructure sectors), and other (e.g., aging infrastructure issues). Game 1 participants were fairly equally aware of physical, cyber and other threats and vulnerabilities, but had little understanding of complexity issues.

Figure 4. Relative weighting of Game 1 solution categories to types of threats



The Game 1 participants' acceptance of specific solution categories were indicated by the following priorities (solution selection frequency indicated within parentheses):

- Create an Infrastructure Assurance Research Institute (20)
- Create a National Indications and Warnings System (18)
- Develop methods for assessing cost/benefit tradeoffs on robustness (13)
- Identify critical nodes (11)
- Develop adaptive software to discern warnings and indicators (10)
- Provide permanent tax credits for infrastructure assurance (10)
- Establish a public/private certification authority and laboratory (10)
- Develop professional licensing standards (e.g., similar to the process for licensing professional engineers) for those that make critical infrastructure decisions (10)
- Set up NCS-NSTAC-like structure for coordination (8)
- Aggressively promulgate warnings of new vulnerabilities (8)
- Establish grants and incentives for R&D to increase infrastructure assurance (8)

As stated previously, these prioritized solution categories, and those from other sources, provide the basis for the Commission's Solution Catalog. The Catalog's solution categories served as a principal input to Game 2 participants for validation.

Solution Drivers and Other Important Considerations

The team discussions and strategic plans identified by the Game 1 participants indicated that the ***awareness of threat varies greatly between security experts and infrastructure practitioners.*** Feedback from several of the teams stressed that, currently, the perceived threat is inadequate to motivate inter-sector collaboration. When a crisis hits, organizations will focus on the protection and recovery of their own critical assets.

In addition, the Game 1 participants identified ***public confidence*** as a key metric to be considered for any infrastructure protection solution. The infrastructure practitioners stated that public confidence is a major target of the terrorist when executing an attack and, as a result, should be a prominent consideration of the PCCIP. It was also pointed out that public confidence is also a strength that may be utilized in order to ride out the effects of any infrastructure upsets.

The cyber threat to each individual infrastructure was seen to be time dependent, ranging from the near term (i.e., current to three years) to the far term (i.e., up to 10-15 years). For example, the Telecommunications Team had confidence in the robustness of the overall telecommunications system to cyber attack. The team's estimate for service disruption experienced by an attack likely would be less than a few hours. The Electric Power Team and the Finance and Banking Team stated that their infrastructures would be addressing solutions to the cyber threat in the near term time frame.

Conversely, the Emergency Services Team believed that due to extensive redundancy in their support systems, the cyber threat to their infrastructure is minimal for the next ten years. It was suggested that provisions be made to raise the awareness within the emergency services sector to the problems of congestion with public networks during emergencies. Likewise, the water services representatives pointed out that, overall, much of the water command and control backup systems would still be handled without much automation for the next few years. As a result, they expressed that the cyber threat to nation's water services is minimal until about the year 2010 time frame. The Oil and Gas Team participants identified physical threat as the greatest threat to the supply end and cyber threat as greatest threat to the distribution end through the year 2010.

As stated previously, there was a lot of feedback by the participants concerning the awareness of the physical threat and the aging infrastructure challenges, however, much of the discussion and the proposed solutions were already well known.

Collaboration is Key to Success

The Game 1 participants expressed that collaboration among public and private infrastructure stakeholders is key to the success of the protection of the nation's infrastructure, however, it is also counter cultural. The participant's provided some suggestions for encouraging collaboration. As an example, cyber threats from foreign governments were rarely (if ever) considered by the infrastructure practitioner during the process of Game 1. It was pointed out that such threats should be adequately defined by the appropriate government agencies before many private organizations would consider them. This process for defining the foreign nation threat might serve as a fundamental focal point for public and private organization collaboration.

It was also pointed out that current models for assessing risk were essentially focused at the organization level or to a specific infrastructure. In order to better address impacts between dependent sectors, integrated models for risk assessment of interdependent sectors should be developed.

Insurers Have a Role in Managing Risks

Game 1 was instrumental in raising the awareness of the insurance industry for their role in the protection of the nation's infrastructure. In particular, the Insurers Team participants were energized to provide products for protection against the exposures of doing business over virtual networks. In order to define and develop such products, however, they identified their need for accurate threat and consequence data.

The insurers team estimated that losses less than those experienced by hurricane and earthquake damage (e.g., less than $25 billion) might be potentially insurable, if the market is sufficiently diversified and motivated. Until the market matures, the insurers team suggested that government resources may have to be identified to cover critical or strategic vulnerabilities of greater than $1billion. It was also pointed out that private organizations and insurers have the major responsibility for addressing protection solutions against cyber threats since attacks by foreign nationals may be indistinguishable from attacks by "benign" sources.

Vulnerabilities Identified by Red Teams

The Game 1 Red Team action proposals raised the awareness of potential threats and vulnerabilities for the Game's participants. The following upset examples represent vulnerability scenarios identified by the Red Teams.

A telecommunications attack example: the Telecommunications Red Team attested to the fact that the telecommunications infrastructure is robust, but it may be vulnerable to an attack by a patient aggressor. A scenario was developed whereby an aggressor could assume a strategic posture for manufacturing critical hardware to be sold to telecommunications companies. The hardware might be encoded for a date-triggered failure (e.g., oscillators fail after a certain time count, etc.). After five to ten years of supply, the sabotaged components would be ubiquitous across the telecommunications network. It was postulated that recovery from such a calculated scenario would take weeks. In addition, the intense focus by organizations in recovering from such an "attack" could divert attention from any of the aggressor's follow-on actions.

A finance and banking attack example: A nation state could launch structured physical and cyber attacks on centers of US financial services and assets to erode the confidence of the public. The agents of a nation state might orchestrate a disinformation campaign against the New York Stock Exchange by injecting erroneous stock information sourced from one or a limited number of news services. This action may be combined with physical attacks on critical financial or banking facilities.

US Infrastructure Assurance Prosperity Game™ 2

The results of the first Game were used to focus the second Game on obtaining detailed response for solutions to the emerging vulnerabilities due to cyber, cyber-related-physical, and complexity effects expected during the next 15 years: from 1997 through 2012.

Game 2 Objectives

The objectives of the second Game were the following:

- Assess the advantages and disadvantages of a variety of solution options for protecting the US infrastructure
- Identify the models for collaboration or key relationships necessary for the protection of the infrastructure
- Provide a clear understanding on missions, roles & functions of organizations that should be involved in these collaborations

Game 2 List of Solution Categories for US Infrastructure Protection

A Solution Catalog, consisting of 22 broad solution categories for US infrastructure protection, was compiled by the PCCIP and Sandia. Each solution category also identified a number of potential options for how the solution might be enacted. The categories with their associated options were presented as "starters" to focus Game 2 interaction and to speed play. These "starters" were not intended to discourage players from devising novel solutions, or from modifying those presented. A number of the categories and options were derived from specific observations, proposals and recommendations of prior bodies that have addressed infrastructure assurance issues. Some of the categories and options were included because they reflect solutions invoked during play of Game 1. Still others appeared in the catalog to stir provocative discussion.

The Game 2 solution categories included (see the US Infrastructure Assurance Prosperity Game™ 2 Handbook, pages 10-22, for a complete description of solutions and associated options):

Vigilance

1. Increase public awareness and education
2. Enrich training programs for cyber-security professionals, consider licensing or certification
3. Mandate administrative and regulatory requirements for government and/or the private sector to promote information system security and early warning of threatening cyber attacks
4. Develop coordinated national infrastructure assurance policies between government and the private sector
5. Encourage coordination of national infrastructure assurance policies within the government
6. Support creation of a permanent infrastructure protection capability
7. Encourage reconsideration of existing federal department and agency jurisdiction and authority
8. Enhance protection, mitigation, recovery, and emergency response capabilities through development and refinement of coordinated emergency response plans
9. Enhance deterrence domestically and internationally

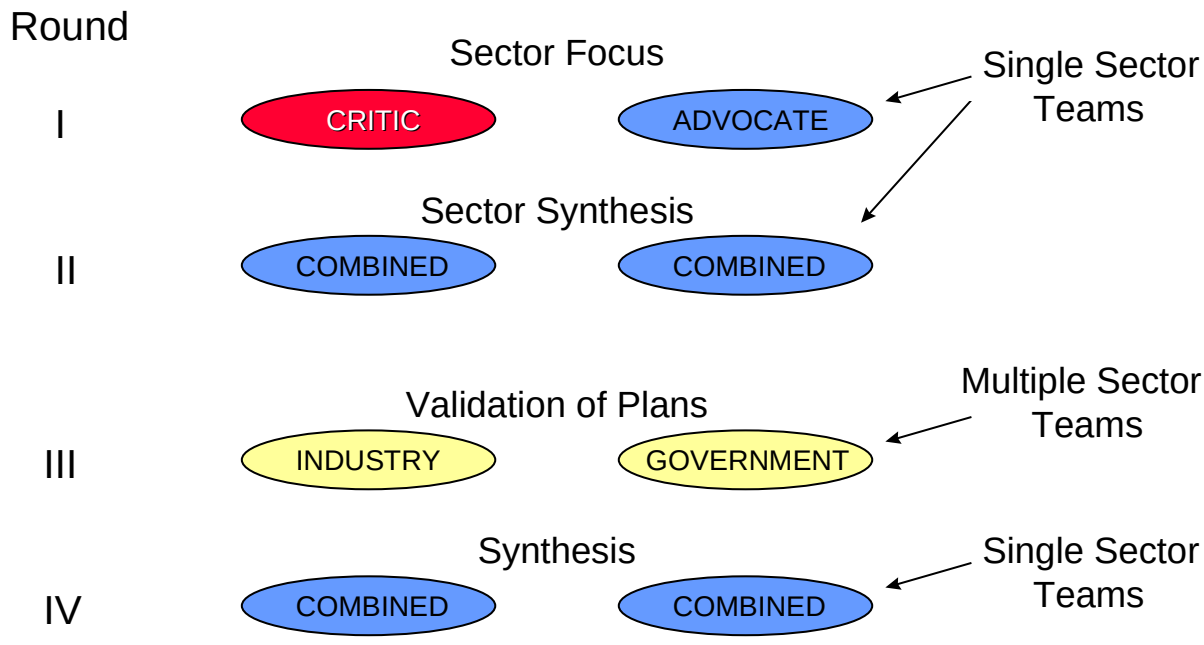
Network Management

10. Develop security *standards* for software, hardware, and network design
11. Develop security *certifications* for software, hardware, and network design
12. Promote international cooperation and participation in assurance practices
13. 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)
14. Support creation of a centralized data collection and analysis capability to further development of an effective indications and warnings system
15. Accelerate reform of the liability climate
16. Support adoption of public-private investment plans and incentives
17. Encourage government efforts to identify, create, and maintain a "minimal essential infrastructure"

Technology

18. Advance specific technology needs and requirements (cyber)
19. Advance specific technology needs and requirements (physical)
20. Promote public-private and government-assisted research and development of specific technology needs and requirements
21. Support mandated adoption of specific technology needs and requirements
22. Develop new risk management tools, models, and techniques

Figure 5. Game 2 Process



Game 2 Design and Process

Lessons learned from Game 1 suggested modifications for Game 2 (see Figure 5, Game 2 Process).

Round 1

In Round 1 of Game 2, teams were organized by Infrastructure (i.e., the combination of industry and government participants responsible for the effective operation of a major element of the services supporting our highly technical society) as Advocates and Critics. The Advocates and Critics detailed the advantages and disadvantages, respectively, of the solutions as applicable to their infrastructure.

See the US Infrastructure Assurance Prosperity Game™ 2 and Planning Event Final Report, Appendix A and B. This is a separate document (dated April 8, 1997) and presented to the PCCIP on April 10, 1997. Appendix A identifies the pre-game infrastructure solution category priorities selected by each infrastructure's Advocate and Critic teams. Appendix B represents the collection of comments for the advantages and disadvantages from the teams for each of the 22 solution categories.

Round 2

In Round 2, the Advocates and Critics of each infrastructure collaborated to define the rudimentary strategic summaries necessary to assure the protection of their infrastructure.

Round 3

In Round 3, the participants were reassigned to Industry Teams and Government Teams; both were comprised of participants from industry and government to enrich the diverse perspective of each. The teams interacted to validate or invalidate rudimentary strategic summaries and policy initiatives by negotiating conditions and support for implementation among the Industry Teams and Government Teams. Each team was provided a budget to use in negotiating their agreements.

See "Financial Resources for Round 3 Negotiations" on page 30 of the Game 2 Player's Handbook. Also, see the US Infrastructure Assurance Prosperity Game™ 2 and Planning Event Final Report, Appendix C. Appendix C presents a summary of the agreements among teams for infrastructure solution priorities.

Round 4

In the Synthesis Session, the Infrastructure Teams were reconstituted (as in Round 2) to capture insights from Round 3 and informally report them to the rest of the team members. The rudimentary strategic summaries were updated by these insights to in order to determine initial strategic plans for each infrastructure team.

See the US Infrastructure Assurance Sector-Specific Solution Plans. This is a separate document (dated April 17, 1997) and sent to David Jones. This document represents the collection of initial strategic plans determined by each infrastructure team.

Prioritized Solution Categories for US Infrastructure Protection

The Game 2 gaming session (Round 3) provided convergence and prioritization of solutions for US infrastructure protection. During this round, the prioritization for solution categories by the players assessments is identified in Table 2.

Table 2. US Infrastructure Solution Category Prioritization

(NOTE: *Solution Categories are prioritized by the percentage of total solution categories selected, **not** by amount of investment and **not** by any vote tabulations*)

Solution Category	Solution #	Round 3 Selection (%)
Data Collection, Analysis, Threat Info Sharing	14	21.2
Enhance Response Capability	8	16.2
Develop Risk Tools, Models, Techniques	22	11.2
Develop Security Standards	10	9.5
Increase Public Awareness & Education	1	7.3
Advance Cyber Technology Requirements	18	4.5
Develop Security Certifications	11	4.5
Advance Physical Technology Requirements	19	4.5
Coordinate Infrastructure Assurance Policy	4	3.9
Infrastructure Assurance Technology R&D	20	3.9
Cyber Training, Licensing, Certification	2	3.9
Coordinate Government Agencies	5	2.8
Enhance Deterrence	9	2.2
Reevaluate Existing Gov. Authorities	7	1.1
Create Permanent Infrastructure Protection	6	1.1
Promote International Cooperation	12	0.6
Accelerate Liability Reform	15	0.0
Support Public-Private Incentives	16	0.0
Mandate Info Security & Early Warning	3	0.0
Establish Gov. Performance Model	13	0.0
Create/Maintain Minimal Essential Infrastructure	17	0.0
Mandate Specific Technology Requirements	21	0.0
Other	23	1.7

Figure 6 (see Appendix A, Prioritization by Rounds: Solutions for US Infrastructure Protection) provides a graph summary of round-by-round solution category prioritization.

Solution Category Prioritization Process

The prioritized solution categories were determined by the number of times each solution category was specified in agreements among teams, *not by voting nor by gaming dollars*. Due to the questions about the Game 1 voting process, the Game Staff determined that the prioritization of solution categories would be completely decoupled from the Game 2 voting process. Voting by the Game 2 participants was used as a qualitative indicator by the Game Staff to identify weaknesses in individual team dynamics. Game 2 voting provided no quantitative input for validation of solutions.

Prioritization of solution categories was also decoupled from the gaming session's (Round 3) dollar allocations. Due to time and game constraints, the Game Staff recognized that the dollar allocations and agreement amounts may not be explicitly accurate. It was also recognized that some solution categories might be over emphasized in priority due to their high cost for implementation. Therefore, the solution category prioritization was based not on dollars, but by the frequency for which the solutions were selected by the teams.

As delineated in the initial strategic summaries and by the presentations at the Game 2 Town Meeting, preferred themes for action were expressed for:

- Data collection, analysis & threat information sharing are the most critical needs (21.2% of solutions selected in investments)
- Response capability: enhance protection, mitigation, recovery, and emergency response capabilities (16.2%)
- Risk management: develop new risk management tools, models, and techniques (11.2%)
- Security standards: develop security standards for software, hardware and network design (9.5%)
- Education & awareness: increase public and stakeholder awareness and education (7.3%)

The following sections provide additional commentary collected from the Game 2 participants concerning the top three solution categories: centralized data collection, analysis, and sharing; enhance response capability; and develop risk tools, models, and techniques.

Centralized Data Collection, Analysis, and Sharing

According to the Telecommunications Team, "… centralized data collection, analysis, and threat information sharing is the 'piece de resistance' of the entire issue (i.e., protection of the nation's infrastructure) … ." All other Game 2 teams also selected and invested in this priority solution category. Team discussions indicated that data collection and information sharing was the fundamental advance leading to a National Indications and Warnings capability.

The difficult, but essential, first step in realizing a collection, analysis and information sharing capability will be to establish trust in sharing of information. The Telecommunications Team pointed out that information sharing procedures must be developed that protect sources and avoid detrimental market responses as a result of a company's divulging proprietary information on attacks. The Team emphasized that "… companies ***will not report intrusions unless anonymity***

is assured… ." This feedback pointed to the need to develop trust between the private sector and government agencies. A specific concern is the reluctance on the part of industry to share vulnerability data with the FBI. The FBI seems to be willing to share threat data, but industry has not taken the initiative to access it.

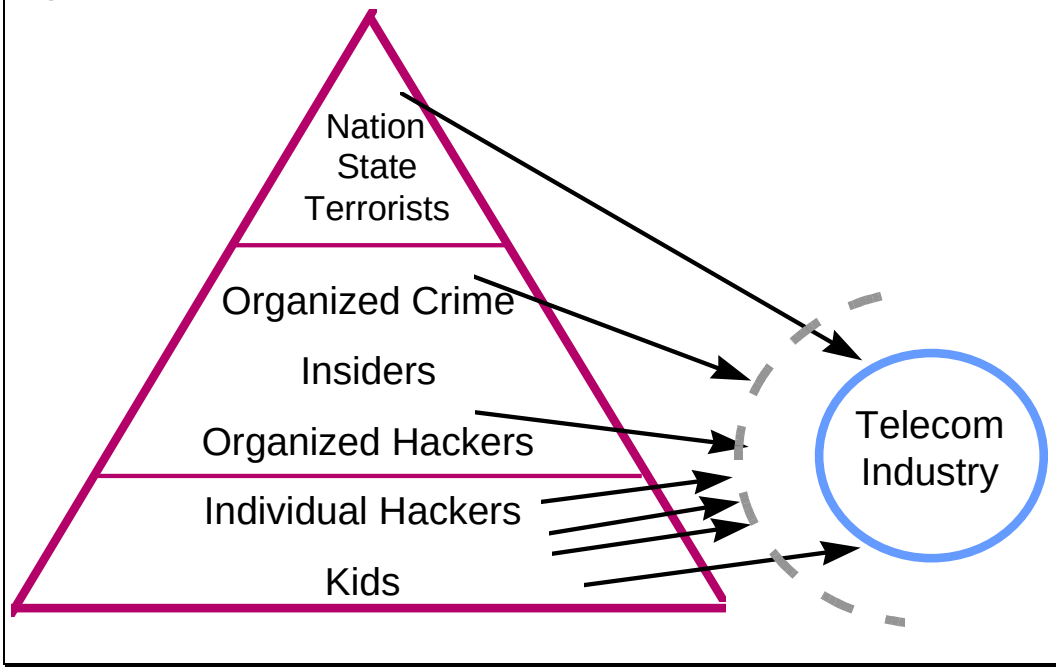
Other important objectives to be addressed in creating a collection, analysis and information sharing capability will be to:

- Clarify responsibilities and appropriate actions with respect to the complexities and interdependencies inherent in an infrastructure(s) under attack
- Promote awareness of industry CEOs to the threat and vulnerability (in addition to any policy initiatives) effects on their business prospects, profits, and potential liabilities

The State and Local Services Team proposed that a centralized data collection, analysis, and sharing effort could be based on a collaboration model such as the Center for Disease Control (CDC). The Team expressed that collaboration should not be limited to only cyber threat and vulnerability. The Team offered that government organizations often do a very good job in data collection and analysis activities, as does the CDC. The Team differentiated the CDC's capabilities, however, in its proactive support and response efforts with local organizations to mitigate or eradicate disease.

The preferred means, identified by the players, for developing a Centralized Data Collection, Analysis, and Sharing capability was to task existing government resources (at existing levels of funding) to develop centralized data collection and analysis capabilities and to share threat information with the private sector.

Figure 7. The source and intent of attacks should be addressed



The Telecommunications Team identified a need to gather and analyze attack data in order to ***determine the source and intent of attacks*** upon the telecommunications infrastructure since "… it is difficult to deduce what is the underlying cause by just observing or experiencing the attack … ." As indicated by the pyramid of potential cyber attackers (ranging from the greater number of "benign" hackers to the lesser number of nation state terrorists) in Figure 7, the telecommunications target is shielded from many of the immediate indicators that might identify the attacker and his/her intent. A collection, analysis and information sharing capability may provide insights to address this issue.

Enhance Response Capability

Improvements in the ability to recover from disruptions was identified by the Game 2 participants as an essential emphasis. All but one team selected and invested in this priority solution category. Several teams pointed to the need for a permanent infrastructure protection initiative which would focus on developing a robust response capability to strategic upsets since all threats can not (or may not) be deterred. Important functions to be addressed by this initiative would include:

- Develop baseline political, human, cyber, and physical threat and vulnerability parameters for the infrastructures
- Examine interdependencies and cascading effects across the sectors
- Develop (where appropriate) capabilities to assure immediate response
- Explore diversification of supply systems to enhance sector(s) robustness

It was readily recognized that the State and Local Services and Law Enforcement Community are already organized to manage elements of recovery, however, it was attested that their capabilities must be improved in order to address selected, strategic level upsets.

Three teams (Transportation, Core Domestic, State and Local Services) aligned to support a senior executive committee to address infrastructure protection issues. The committee (i.e., "Consequence Management Umbrella") of senior executive infrastructure stakeholders would provide recommendations for improving infrastructure protection, mitigating attacks and effects, and improving recovery and emergency response. Their reports would be disseminated to the represented sectors as well as to the National Security Council, which in turn, would report them to the President.

The Finance and Banking Team noted the particular vulnerabilities of, and threats to, increasingly complex information systems. They identified the need to improve the recovery capabilities for attacks against these systems. The Team supported that establishment of an NSTAC-like organization to specifically address ***information systems threat and vulnerability and recovery mechanisms***.

Develop Risk Tools, Models, and Techniques

Participant feedback indicated that improved risk management capabilities should provide informed, standards-based certification of facilities and critical systems. In addition, such

capabilities would drive research and development to meet escalating threats and vulnerabilities through the following activities:

- Estimate risk through comprehensive assessment process
- Develop and establish effective and appropriate standards
- Provide guidelines for certifications
- Drive risk-averse technology development and deployment

Feedback from the participants indicated that the government has an important role in the development of risk management tools, models and techniques. As an example, the Electric Power Team suggested that government partners should fund the infrastructure research and development component to assure that strategic assurance goals are met. The Transportation Team stressed that the government has a very important role in identifying the critical infrastructure nodes to be protected from a strategic viewpoint.

The preferred means, identified by the players, for developing risk tools, models and techniques were to:

- Support the establishment of a joint government/private sector institute to study and develop new risk management models
- Develop risk tools, models and methods that support system designers' decisions effecting system-level robustness and in economic selection studies

Priority Issues Effecting Opportunities for Action

The Game 2 participants identified three fundamental drivers that would determine the success of and effect the opportunities for acting on the preferred solutions to protect the nation's infrastructure:

- Industry and government ***partnership*** is essential
- Effective and appropriate ***leadership*** must be established for protection of the infrastructure
- ***Threat*** must be ***validated*** in terms of cost and impact prior to substantial industry investment

Partnership

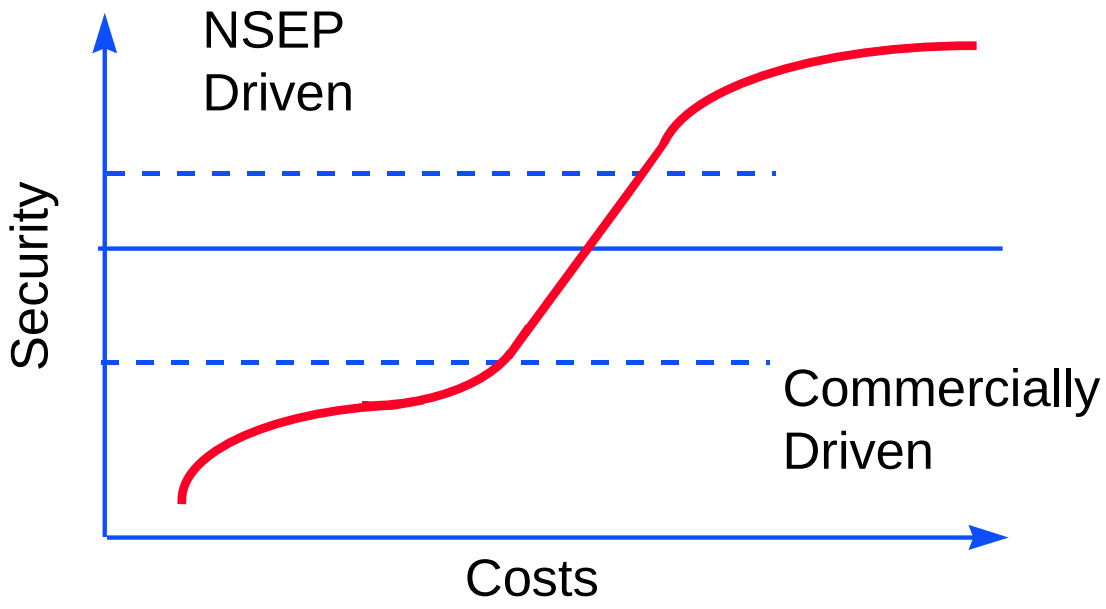
Separate team discussions converged on the necessity of industry-government partnership to address the emerging threats and vulnerabilities. The infrastructures are essentially owned and operated by industry, and regulated by government. Government has complementary capabilities in intelligence gathering, legal sanctions, and enforcement that may be beneficial to industry. It was stressed that partnership should provide *Broad Performance Goals* and not detailed operational interventions.

The strategic planning summaries detailed by the separate infrastructure teams revealed several important issues requiring collaboration between industry and government before development and/or implementation of infrastructure protection policy.

- **Industry Should Lead** in any public/private partnership in order to respond to market forces, especially after the start-up phase when market forces mature. It was pointed out that the competitive forces of industry will inevitably drive advances in technology; regulators should not lock out new technology evolution.

  The Telecommunications Team provided a graph illustrating various levels of infrastructure security. The Team pointed out that industry currently addresses security according to market demand (see commercially driven level of security in Figure 8). The Team stressed that the legitimate drivers for government action are the definition of national security and emergency preparedness security (NSEP) requirements (see NSEP driven level of security in Figure 8) and the funding of initiatives to develop strategic levels of security.

Figure 8. Levels of Infrastructure Security



- **Reform Liability** to address jurisdiction and shared liability in cyberspace.
- **Coordinate Policy Analysis and Review** with the established procedures of the stakeholders. Reform procedures (where appropriate) to handle the interdependencies among infrastructures.

Models for Collaboration

The partnership models preferred by private organizations emphasized the ***development of trust*** and a limitation on the operational interventions by government.

National Security Telecommunications Advisory Committee

By far, the President's National Security Telecommunications Advisory Committee (NSTAC) was the most frequently cited model for infrastructure protection collaboration between industry and government. It was apparent that the NSTAC enjoys an excellent reputation spanning

several infrastructure sectors. For example, the Transportation Team noted that the "… NSTAC is a good example of a joint body with strong industry representation. It's also good because it coordinates only at the highest, most abstract levels." The Telecommunications Team promoted the NSTAC to address infrastructure protection challenges since the "… telecommunications industry does not want another overseeing commission or regulatory agency to solve infrastructure issues." In addition, the Electric Power Team suggested a central organization, similar to NSTAC, to assume the lead in protection of the electric power infrastructure. The Team stated that such an organization would be best placed under the North American Electric Reliability Council's (NERC) umbrella.

Super Federal Advisory Committee (FAC)

Several teams (i.e., White House, Electric Power, Core Domestic, Core International, Defense, Law Enforcement Community, Telecommunications) contributed to a concept calling for the organization of a Super FAC to address the nation's infrastructure protection challenges. The Super FAC would consist of information systems, telecommunications, and electric power CEO's to address sector specific and interdependent issues. The Super FAC would report to the White House via either the National Security Council (NSC) or the National Economic Council (NEC).

Minimal Essential Infrastructure Collaboration

The Finance and Banking Team suggested an incremental approach to address US infrastructure protection by proposing a model for collaboration to assure a minimal essential infrastructure. It was suggested that the creation of a cross-sector, industry-led model for collaboration should develop:

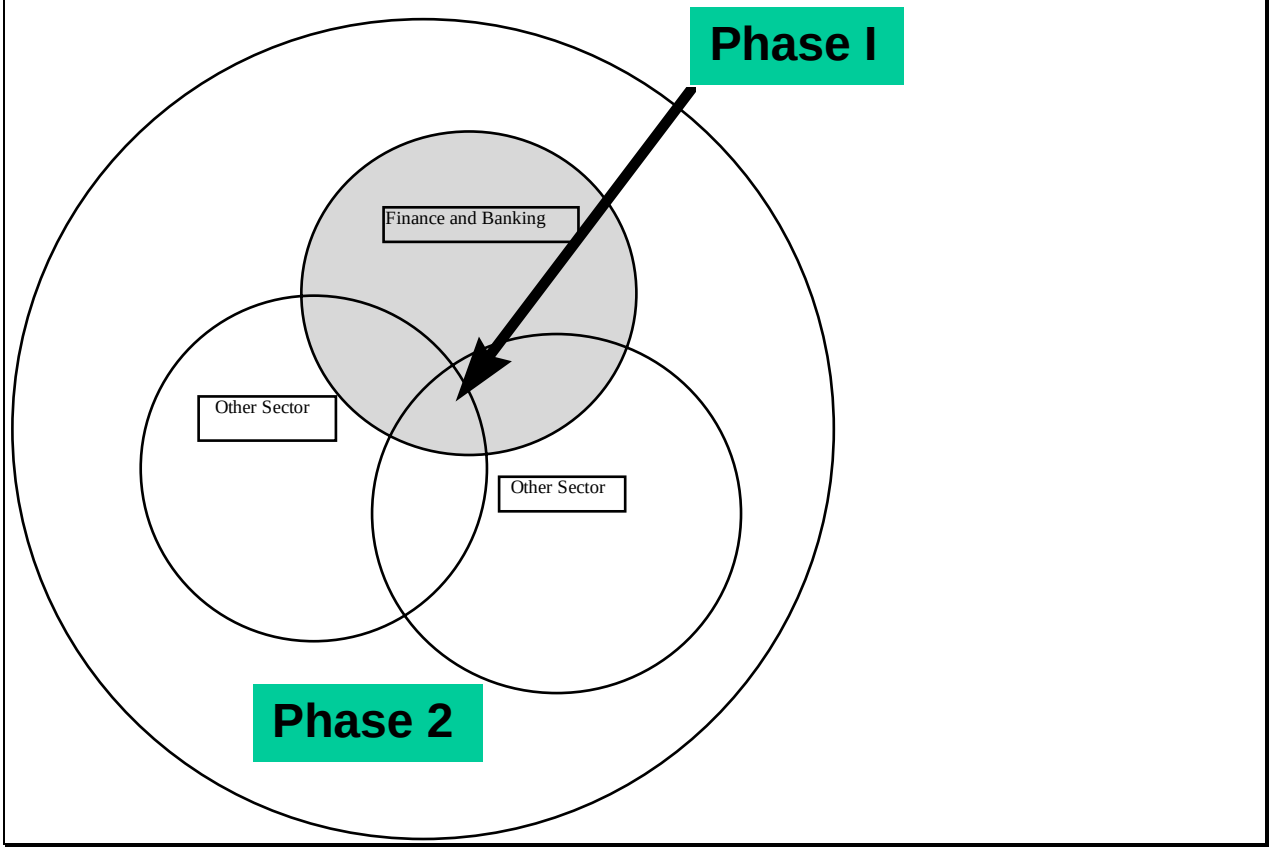
- Vision and policies
- Best practices and procedures
- Standards and certifications
- Risk management tools, models and techniques
- Response capabilities

The *Minimal Essential Infrastructure* approach might initially address the Finance and Banking, Electric Power and Telecommunications infrastructures.

The Finance and Banking Team expressed the need for the establishment of standards as an important initial step to assure a minimal essential infrastructure. ***Certifications can not be implemented without standards***. Standards definition and introduction would be addressed in two phases (see Figure 9):

- Phase 1: Identify potential overlaps between sector standards. Design standards which apply to sectors ONLY in overlap. Each sector would also have standards which apply only to them.
- Phase 2: Identify "universal" standards (e.g., digital certificate standards) which would apply to all infrastructures.

Figure 9. Establish Standards for Minimal Essential Infrastructure



Effective and Appropriate Leadership

Much of the Game 2 participants' commentary concerning leadership focused upon the role of the government. The distinguishing feedback from the Game 2 participants indicated that government may have to seed protection initiatives until the commercial market matures to address strategic levels of protection. Also, the current lack of effective and appropriate government leadership is a major impediment to infrastructure protection.

The Electric Power Team suggested that government partners should fund the infrastructure research and development component so that threat and vulnerability information is not perceived as proprietary. They also pointed out the government's role is to help establish national trends and policy derived from the information sharing between industry and government: without falling into a "big brother" role. The Transportation Team stated that the government's role is to identify what the minimal infrastructure protection requirements are; the telecommunications sector will not lead.

The Transportation Team also stressed that a common vision and a clear definition for cooperative roles must be established for government agencies having responsibility for infrastructure protection. The State and Local Services Team attested that turf battles between

government agencies are seen as the biggest impediment to any success for infrastructure protection. The Team indicated confidence in the FBI, however, several sectors feared the FBI having a central role in infrastructure assurance.

Several teams voiced similar concerns for other government agencies. For example, it was pointed out that FEMA needs to demonstrate a more collaborative, higher technology behavior to improve its credibility with the infrastructure sector stakeholders.

Several teams indicated that the White House was not the optimal choice as leader for infrastructure protection. It was pointed out that "… the appropriate role of the White House should be to review all proposed solutions to ensure that they have sufficient private sector support, are not overly reliant on government in terms of either funding or agency support, and that any necessary government alliances have been specified, solicited, and approved."

The Finance and Banking Team provided a summary statement concerning government's role in infrastructure protection, "… the dichotomy follows: there is an aversion to government, but government is expected to take a lead or have a major role. Therefore, the most appropriate ***government role is that of facilitator***."

Status Following the US Infrastructure Assurance Prosperity Games™

At the conclusion of the US Infrastructure Assurance Prosperity Games™, Sandia National Laboratories has provided important assessments from a broad cross-section of infrastructure stakeholders to be considered by the deliberations of the President's Commission on Critical Infrastructure Protection (PCCIP).

The following objectives have been addressed:

- *A prioritized list of US infrastructure protection solution categories has been identified*
- *Fundamental drivers that will determine the success of (as well as effect the opportunities for acting upon) the preferred solutions to protect the nation's infrastructure have been detailed*
- *Potential models for public/private collaboration to address the protection of the nation's infrastructure have been proposed*
- *The relative awareness of the infrastructure practitioner to the vulnerability of the US infrastructure to the cyber, physical and complexity threats has been measured*
- *There has been an increased interest and participation (over 175 persons) from the US infrastructure practitioners and security experts communities to address protection challenges*

Appendix A: Prioritization by Rounds: Solutions for US Infrastructure Protection