

# CRITICAL INFRASTRUCTURE PROTECTION STRATEGIC SIMULATION 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, Booz-Allen & Hamilton. 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**

- I. STRATEGIC SIMULATION FOR THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (PCCIP)**
- II. INDUSTRY CONCERNS AND RECOMMENDATIONS**
- III. INSIGHTS AND OVERVIEW OF INDUSTRY SECTORS**
- IV. GOVERNMENT TEAM INSIGHTS**
- V. SIMULATION OBSERVATIONS**
- VI. NEXT STEPS**

**THE PCCIP STRATEGIC SIMULATION PROVIDED AN OPPORTUNITY FOR THE COMMISSION, GOVERNMENT AND INDUSTRY PARTICIPANTS TO EXAMINE THE EFFECTIVENESS OF ITS PROPOSED POLICIES AND PROCESSES TO PROTECT THE NATION'S CRITICAL INFRASTRUCTURES AND PROMOTE ECONOMIC OBJECTIVES**

- **PCCIP SPONSORED THIS SIMULATION—WITH PARTICIPATION BY BOTH GOVERNMENT AND INDUSTRY LEADERS—TO CRITICALLY ASSESS THE COMMISSION'S POTENTIAL RECOMMENDATIONS**
- **THE OBJECTIVES OF THE SIMULATION WERE TO ASSESS ALTERNATIVE APPROACHES TO TWO KEY QUESTIONS:**
  - How can national security, economic competition and societal benefit be promoted through U.S. policy regarding the critical infrastructures?
  - How should the relationship between Government and business be established to promote mutual objectives?

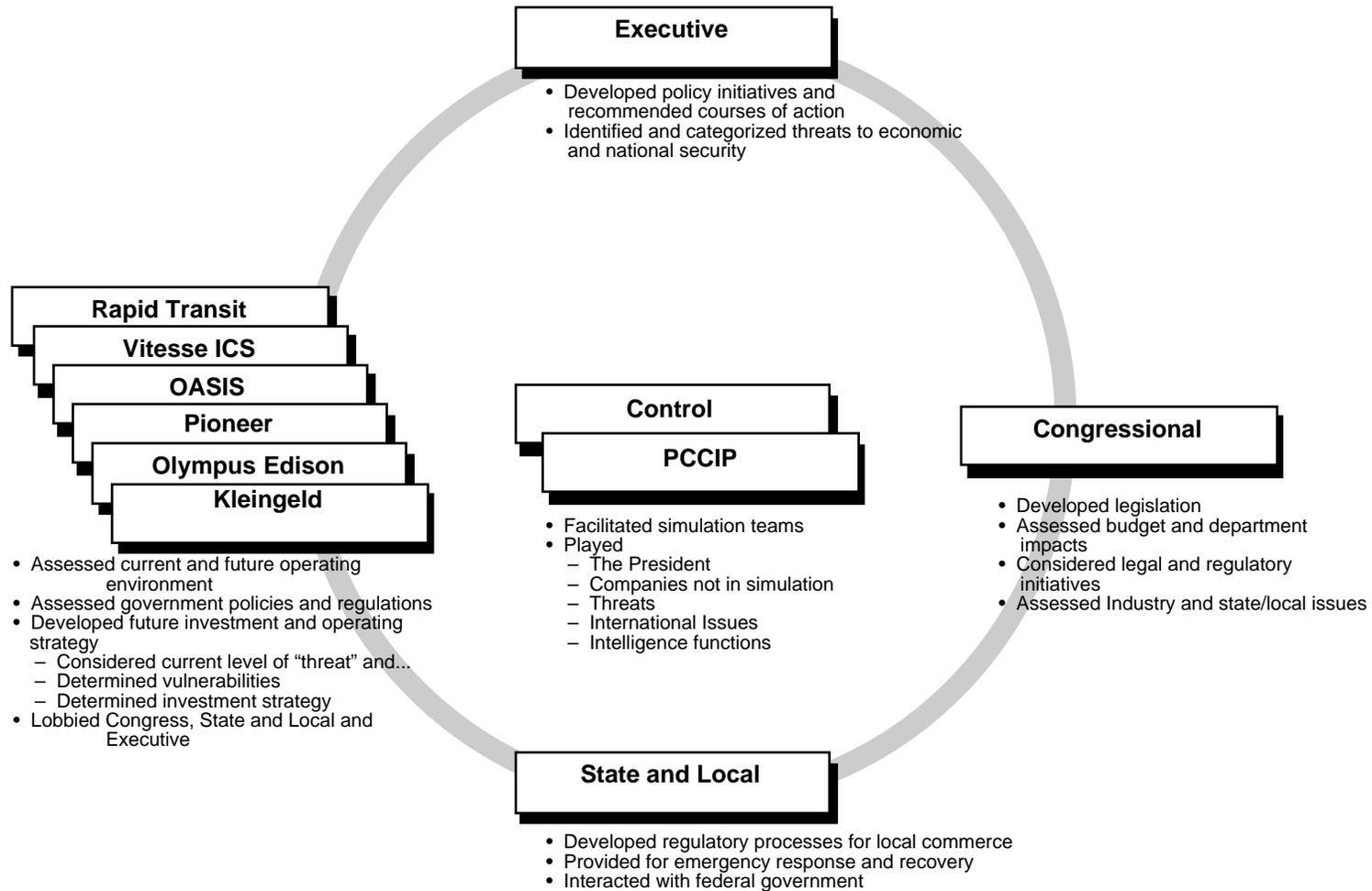
## **THE COMMISSION PROVIDED DRAFT RECOMMENDATIONS FOR CRITICAL INFRASTRUCTURE PROTECTION TO REDUCE VULNERABILITIES AND TO BE ABLE TO ADDRESS POTENTIAL THREATS**

- Develop a new, streamlined Federal Agency which would be responsible for alerting the owners, operators, and users of critical infrastructures to existing or potential threats
- Set standards for security (in concert with Industry) and negotiate agreements with other countries dealing with security standards
- Define increased liability requirements of critical infrastructure owners and operators for service failure when standards have not been met
- Provide Federal assistance in enhancing information and communications security while promoting the development of private sector initiative
- With Industry advice, identify technology needs to assure critical infrastructures' security; transfer existing technology already in Federal hands to Industry and fund needed development
- Support a private sector organization to certify products and accredit practitioners in critical infrastructure assurance

**THE COMMISSION PROVIDED DRAFT RECOMMENDATIONS FOR CRITICAL INFRASTRUCTURE PROTECTION (CONTINUED)**

- Administer a series of direct incentive programs, consisting of technology transfers, loan guarantees, etc., designed to motivate business investment in infrastructure protection
- Expand the Federal role in enforcing laws designed to protect critical infrastructures and negotiate international agreements to facilitate the investigation and prosecution of cyber crime
- Promote the awareness of the general public and Industry's awareness of the need to increase attention to critical infrastructure security
- Increase training opportunities for owners, operators and users of critical infrastructure in detecting and countering intrusions and in mitigating their effects

**TEAMS REPRESENTING CONGRESS, THE EXECUTIVE BRANCH, STATE GOVERNMENT, AND 6 “REPRESENTATIVE” COMPANIES – REPRESENTING THE SIX SECTORS OF TRANSPORTATION, TELECOMMUNICATIONS, UTILITIES, HEALTHCARE, WATER, BANKING AND FINANCE - INTERACTED OVER 3 DAYS**



## THE SIX INDUSTRY TEAMS WERE REPRESENTATIVE OF KEY NATIONAL INFRASTRUCTURE SECTORS

COMPANY	DESCRIPTION
<b>OASIS</b>	OASIS provides water services to the City of Los Angeles. Services are provided to over 640,000 customers in the City of LA. Over 75% of that water comes from the watershed areas of the Eastern Sierra Mountains. 15% of the water comes from ground sources in the San Fernando Valley and the remaining 10% is purchased from the Metropolitan Water District of Southern California. OASIS provides on average of 580 million gallons of water per day to the city of Los Angeles to satisfy the daily 188 gallon per person demand. To tap the necessary water supplies of the Eastern Sierra mountains an aqueduct system was developed in 1940. Today that system has extended to over 330 miles of aqueducts capable of moving 430 million gallons of water per day.
<b>Vitesse ICS</b>	Vitesse ICS owns, operates, and maintains wireline and wireless communications networks for the local and long-distance transmission of voice, data, and video. Devises markets, and provides electronic communications products and services for a diverse range of domestic and international residential, Government, and business clients. Products and services offered include POTS, enhanced wireline services, cellular services, personal communications services, paging and specialty mobile services, Internet access, interactive video, and directory services.
<b>Pioneer</b>	Pioneer Inc., is the nation's largest provider of healthcare services with facilities in 38 states, as well as, recent investments in international facilities in England, Switzerland, and Spain. Pioneer's network includes 331 hospitals, 129 surgery centers, more than 565 home health locations, and a nationwide pharmacy benefit management company. One of Pioneer's key assets, is the electronic patient record system. Pioneer maintains the largest database of inpatient and outpatient electronic patient records. During the last year, significant resources have been targeted toward the initialization of an intranet "telemedicine" network.
<b>Kleingeld</b>	Kleingeld Bank, headquartered in New York City, is the nations largest bank company with over \$300 billion in assets. Kleingeld, offers both retail and wholesale services, but has since expanded into a wider range of financial services to include private banking, corporate financing, debt and equity underwriting, foreign underwriting, mortgage banking, credit cards, U.S. corporate and international banking and investment services. In order to offer this range of financial services, Kleingeld is a member of Industry utility organizations, to include SWIFT, CHIPS, the Federal Reserve, Depository Trust Company and the major exchanges .
<b>Rapid Transit</b>	Rapid Transit is the largest fully integrated transportation company in the United States servicing 45,000 communities nationwide. Headquartered in Chicago, Illinois, Rapid Transit has an extensive fleet of aircraft, trucks, and ships to transport cargo to more than 185 countries around the globe. Rapid Transit has made extensive use of advanced computer and communication technologies including global positioning satellites, on-line communications, and EDI capabilities for tracing, tracking, documentation and billing. This extensive reliance on advanced technologies has enabled Rapid Transit to provide more comprehensive and faster service with a greater reliability.
<b>Olympus Edison</b>	Olympus Edison is one of the nation's largest investor-owned electric utilities. It generates, transmits and distributes power to 1.5 million residential and commercial customers in the Atlanta, Georgia, area. In addition, it offers wholesale power sales nationally. Olympus Edison owns and operates a system of nuclear, coal, oil, natural gas and hydroelectric power stations. The distribution of these sources is as follows: 51% coal, 20% nuclear, 15% gas, 8% hydroelectric, 3% oil and 3% purchased power. The variety of power stations allows Olympus Edison to ensure system reliability, and service to customers, in case of a major problem in one of these areas. In 1996, Olympus Edison has total electricity sales of 52.4 billion kwh, with 17.7 billion kwh in residential sales. Olympus Edison is regulated by the Public Service Commissions of Georgia; the Nuclear Regulatory Commission; and the Federal Energy Regulatory Commission.

**INDUSTRIES BELIEVE THEIR ABILITY TO PROTECT THEMSELVES AGAINST TODAY’S THREATS IS ADEQUATE. HOWEVER EMERGING TECHNOLOGY AND INDUSTRY DEREGULATION PROVIDES AN INTERDEPENDENT SYSTEM WITH NEW POINTS OF VULNERABILITIES AT A TIME WHEN NEW THREATS ENTER THE INFORMATION AGE**

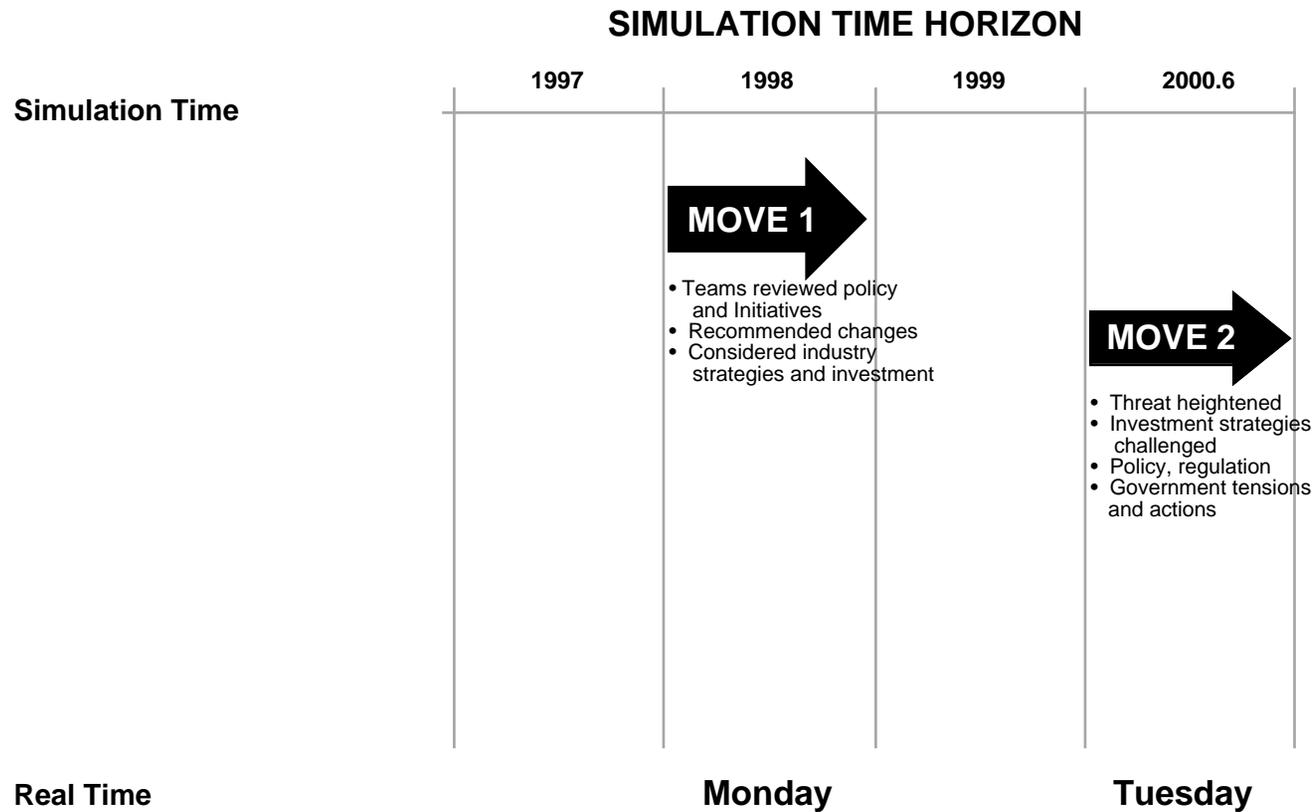
- Industry teams were presented with a series of escalating threats designed to test the Commissions recommendations and challenge industry decision makers to invest and seek assistance in infrastructure protection

<p><b>Government Policies Move 1</b> Information Sharing Technical Assistance</p>	<p><b>Threat Environment</b> Hacker Intrusion Indications of bigger threats</p>
<p><b>Government Policies Move 2</b> Technical Assistance Liability Emergency Response</p>	<p><b>Threat Environment</b> Inside-Outside Threat An increased “Cyber” Threat Physical Terrorism</p>
<p><b>Government Policies Move 3</b> Information Sharing Technical Assistance International Agreements</p>	<p><b>Threat Environment</b> Increased Inside-Outside Threat Offshore cyber crime</p>
<p><b>Government Policies Move 4</b> Technical Assistance Emergency Response Reconstitution</p>	<p><b>Threat Environment</b> State Sponsored Threat Offshore origin of thefts Chem/Bio terrorism</p>

Strategic Simulation ...

**THE SIMULATION WAS PLANNED IN A SERIES OF 2 MOVES OVER 3 DAYS—EACH MOVE REPRESENTED 1 TIME PERIOD**

- Move 1 examined commission recommendations with current infrastructure threats



- Move 2 examined globally connected infrastructure, deregulated energy networks and a new Air Traffic Control system against more organized, technically capable threats

Strategic Simulation ...

**INDUSTRY TEAMS WERE TASKED TO ASSESS STRATEGIES FOR PROTECTING THE INFRASTRUCTURE. THE INDUSTRY TEAMS' FINDINGS WERE EVALUATED AGAINST:**

- **The current environment** of the Industry (as well as trends and issues currently facing the Industry e.g., deregulation, international competition, downsizing, etc.)
- **The vulnerabilities and threats** which serve as plausible scenarios with operational and economic impacts, and can effect public confidence for the Industry
- **Competing financial demands** of the companies, including the costs of increasing the protective levels in the infrastructure, as well as the costs associated with loss of public confidence, and assessed vulnerabilities
- **The emergency response** and recovery capability of the critical infrastructure sectors together with federal, state, and local government agencies

**THE FOLLOWING IS A COMPILATION OF THE INDUSTRY PLAYER'S OVERALL VIEWS DURING THE SIMULATION AND DURING THE POST GAME INTERVIEWS WITH SELECTED PARTICIPANTS IN RELATION TO THREATS ON THE CRITICAL INFRASTRUCTURE AND OVERALL SUGGESTIONS ON HOW TO IMPROVE THE CRITICAL INFRASTRUCTURE**

**INDUSTRY IS CURRENTLY FACED WITH THE OPTION OF PROTECTING THEIR OWN INFRASTRUCTURE OR ACCEPTING GOVERNMENT REGULATIONS AIMED AT MANDATING PROTECTIVE MEASURES. BOTH OPTIONS HAVE INDUSTRY CONCERNED**

- Government does not currently provide Industry with adequate information on threats and risks
- Information sharing deficiencies highlight need for new processes as the current structure is inadequate
  - Information flows from Industry to Government (e.g., security problems)
  - Very little information in a form usable to management flows from Government to Industry (e.g., early warnings about possible terrorist activities, and forecast threat analyses)
- Industry feels that the traditional DoD and Intelligence agencies are not structured/equipped to share threat data with Industry
  - Representatives from the six industries shared numerous instances of law enforcement agencies withholding potentially relevant threat data or collecting data from the organizations in question and not sharing results/outcomes
- Industry is concerned that increased regulation will lead to increased operating expenses due to:
  - Reporting requirements
  - Increased investment in technology
  - Increased security measures
- Regulatory requirements cause problems:
  - Regulation may result in increased costs for Industry
  - Regulations are slow to respond to the changing environment
  - Regulations can produce proprietary problems

**INDUSTRY RECOMMENDATIONS TO THE PCCIP WERE MORE CLEARLY DEVELOPED AFTER THE UNDERSTANDING OF A REAL THREAT WAS HEIGHTENED. INFORMATION SHARING, EDUCATION, AND INCREASED RESEARCH AND DEVELOPMENT WERE AT THE FOREFRONT OF THOSE RECOMMENDATIONS**

- Information sharing is essential and must be conducted on a voluntary basis to identify existing vulnerabilities and potential threats
  - There is a perception that Government is not divulging all they know about the threat
  - Industry is reluctant to share proprietary data with Government agencies
- Government’s proposed process for Industry to participate in “information sharing” needs to be better defined
  - A feedback mechanism needs to be established for information sharing
  - Government must establish mechanisms to ensure proprietary data is not released and it is non-attribution (no company names provided)
  - Ensure a level playing field - all competitors must provide the same level of information, and small businesses must be included
  - Clarify which agency or committee will have overall responsibility for the information
- Industry prefers to build on existing mechanisms and organizations. If this is not possible, Industry would like to provide input into, and play an active role, in the development of regulations
  - If a new agency is needed, the Industry wants to actively participate in the development and ongoing activities of the new agency

## **GOVERNMENT MUST GAIN THE TRUST OF INDUSTRY THROUGH A OPEN, HONEST INFORMATION SHARING EFFORT**

- Develop a shared information mechanism between Government and Industry representing the transportation, water, power, telecommunications, banking, healthcare sectors and Government agencies like NSA, FBI, CIA etc. This Industry/Government partnership must be value-added and based on trust. This trust is fostered through free and open communication
  - The ultimate goal is stability and continuity of critical infrastructures via education and awareness in these areas:
    - .. Development and maintenance of current “day to day” Industry security
    - .. Long range planning
    - .. Response to escalation of crisis mode
  - The mechanism should serve as a single point of contact for Industry to obtain vulnerability and threat information. Its mandate would be to focus on critical infrastructure issues and interdependencies between these industries
  - Provide early warning on critical threat data to Industry for risk management. Also develop emergency response capabilities
  - Structure of mechanism:
    - .. Associations have a “seat” and are represented by certain companies on an annual, rotating basis. Selection is based on a set criteria per each Industry sector
    - .. Participation should be inclusive not exclusive and all participants should sign non-disclosure agreements among each other
    - .. Participants make an investment of time and money to ensure Industry “buy-in”
  - Conduct analysis and risk assessments and transfer this information to Industry
  - Coordinate data transfer among Government agencies and Industry associations

**RESEARCH AND DEVELOPMENT HAS BEEN A CONCERN FOR INDUSTRY FOR MANY YEARS, AND THE FEDERAL GOVERNMENT SHOULD TAKE A MORE ACTIVE AND INVOLVED ROLE**

- Government should assist in R&D efforts for interdependent Industry issues
  - Industry needs as much information from Government, in a usable form, as soon as possible to mitigate any threats or vulnerabilities and to identify trends
  - Incentives must be provided from Government (e.g., tax credits) if Government requires higher levels of protection than is required for normal business practices
- The Industry teams felt that the Government possesses the best technical expertise in information security and that expertise needed to be made accessible to Industry. Government should:
  - Provide assistance in developing Industry led security standards
  - Transfer existing security technology
  - Sponsor R&D to develop protective technologies
- Government could expand the role of NSA penetration testing in key infrastructures
  - Should also consider a role for NSA in supporting test and certification of Industry standards
- Government should conduct a credible analytical process of the vulnerabilities and threats
  - Need specific numbers: probability of occurrence and cost prevention estimates for identified threats
  - Industry needs this information before they commit resources
  - Identify points-of-entry for attacks on the infrastructure

**RESEARCH AND DEVELOPMENT HAS BEEN A CONCERN FOR INDUSTRY FOR MANY YEARS,  
AND THE FEDERAL GOVERNMENT SHOULD TAKE A MORE ACTIVE AND INVOLVED ROLE  
(CONTINUED)**

- In the long term, government needs to develop improved security measures
  - Conduct security audits, sponsor testing and verification studies
  - Offset Industry costs to improve security by providing incentives which reach a defined “best-in-class”, security level
  
- Structures do not need to be changed or adapted; however, intra-agency communication within the Government needs to be increased and made more efficient
  - All industries need to incorporate cross-Industry risks into their strategic planning

**TO MAINTAIN INFRASTRUCTURE SECURITY THE FEDERAL GOVERNMENT HAS SUGGESTED AN INFORMATION SHARING MECHANISM. INDUSTRY, THOUGH INITIALLY SKEPTICAL, PROVIDED A SERIES OF CONCRETE SUGGESTIONS**

- Industry felt that the primary Government role should include information sharing, coordination, information exchange and education
  - In doing so, Government should attempt to work through existing Industry organizations/associations
- Government should share threat/intrusion/vulnerability data with Industry to assist in their existing risk management process
- Industry representatives felt that there would be benefit to sharing information between and among the critical infrastructures
  - The team proposed a three tier structure with Industry voluntarily feeding sanitized data into an Industry organization/association who in turn feeds data into national information coordinating activity
  - Industry must see benefit from this activity i.e., a two-way information flow to encourage participation
  - Due to the speed of these events this mechanism must happen at near real-time
- Lack of appropriate threat information from the Government results in an inability to develop appropriate risk assessment model and countermeasures

**THE ONE COMMON THREAD BETWEEN INDUSTRIES IS THE NEED TO SUSTAIN PUBLIC CONFIDENCE IN THE CRITICAL INFRASTRUCTURE. BOTH INDUSTRY AND THE GENERAL PUBLIC MUST BE EDUCATED ABOUT THE THREATS TO THE INFRASTRUCTURE. EDUCATION IS ONE VEHICLE THAT CAN ACTIVELY PROMOTE THE INFRASTRUCTURE SECURITY AND PROTECTION**

- Use trade associations as a vehicle to educate the public on infrastructure threats as well as sources for information to the Government
- Promote seminars and classes through the education system to develop a workforce that will not be susceptible to foreign or domestic intruders to the infrastructure and instill a instinct of public service (i.e. bankers and engineers, like other professional service providers, should have codes of conduct)
- Provide grants to education systems for the development of infrastructure protection systems

## **THE INDUSTRY TEAMS VOICED COMMON CONCERNS AND SOLUTIONS IN RELATION TO INFRASTRUCTURE PROTECTION, BOTH DURING THE GAME AND AT THE FOLLOW-UP INTERVIEWS**

- Common concerns
  - Who pays for the increase in infrastructure protection?
  - Liability for attacks on the infrastructure
  - The creation of another government regulatory agency in an environment perceived as already over-regulated
  - The desire for Industry based standards vs. government requirements or standards
  - The issue of law enforcement reaction to infrastructure attacks
  
- Common solutions
  - Increased, government sponsored, education on infrastructure threats
  - Increased Government funding for R&D technology to protect infrastructure
  - Government-funded incentives for Industry led initiatives to protect their infrastructure
  - Increased two way communication on threat specifics
  - The formation, or expansion of a National Infrastructure Coordination Center (NICC) or equivalent agency that contains Government (Federal, State and Local) as well as Industry representation

**THE FOLLOWING SECTION CONTAINS AN INDUSTRY SPECIFIC PERCEPTION ON INFRASTRUCTURE THREATS AND SPECIFIC SOLUTIONS TO SAID THREATS**

**THE OASIS TEAM WAS CONFIDENT OF THEIR ABILITY TO USE THE EXISTING RESPONSE PLANS IN CONJUNCTION WITH STATE AUTHORITIES**

- The infrastructures which support the water supply Industry are largely independent and therefore less susceptible to direct nation wide threats. The greatest current threat is presented by a physical attack on a specific data system and cyber threats directed against other elements of the infrastructure
- While a particular threat with cascading effects across the country is highly unlikely, the affects of an attack on the water Industry present serious consequences which affect public confidence
- Due to the expansive watershed areas from which water supply companies draw their water, it is virtually impossible to actively protect all suppliers from a terrorist attack
- The water resources are protected from many biological or chemical threats by dilution of contaminants providing the water flows into and through the processing and filtration system
- The water supply Industry is now adequately regulated by federal and state legislation to protect the water supply, mandate water quality, and oversee discharge processes

**WATER SUPPLY COMPANIES OPERATE INDEPENDENT INFRASTRUCTURES IN A MONOPOLISTIC ENVIRONMENT, THUS CREATING AN INDUSTRY WITH SPECIFIC NEEDS**

- The water Industry is more concerned with how an attack on other infrastructures, i.e., banking, telecommunications and power, will effect the water supply
- Existing government agencies effectively regulate water supplies. Government should utilize existing agencies and legislation to protect the infrastructure
- Government sponsored R&D can improve detection and treatment processes for the water Industry

**OASIS IS INTERESTED IN DEVELOPING BETTER AVENUES FOR EMERGENCY RESPONSE BETWEEN INDUSTRY AND STATE GOVERNMENT. THE FEDERAL GOVERNMENT SHOULD HAVE A LIMITED ROLE IN REACTION TO A SITUATION, THEY CAN HOWEVER PROVIDE MANY SERVICES TO THE WATER SUPPLY INDUSTRY**

- The government should provide Industry information concerning the real threats and vulnerabilities to the infrastructure
  - Grant clearances to Industry security personnel so they can know the threats which face their companies
  - Develop interchange between military agencies, the creators of viruses and chemicals, and let water Industry know what agents pose threats to the water supply
- The water Industry believes that the need to replace the aging infrastructure is the most critical current problem
- Sponsor technology transfer and research into rapid detection, investigation and responsiveness to biological, toxic, or cyber threats

**THE WATER INDUSTRY CONSIDERED THE AGING INFRASTRUCTURE THE GREATEST THREAT TO THE INDUSTRY. THEREFORE, THE FOLLOW-UP CONCENTRATED ON WAYS TO PAY FOR THE SYSTEM REPAIR AS WELL AS WAYS TO RESPOND TO EMERGENCIES OR ATTACKS**

- Sequester 5% from the budget for infrastructure improvement on a regular basis for maintenance and repair; process should remain constant
- Creation of more State Revolving Funds (SRF's) to pay for infrastructure repair. This is currently used in large cities but should be expanded to include smaller communities
- Further development in Standardized Emergency Management Systems to deal with natural emergencies, telecommunications and power
- Support and increase the use of volunteer systems in response to attacks, this promotes awareness and accrues costs only when used

**THOUGH THE WATER INDUSTRY AND ITS INFRASTRUCTURE IS LARGELY REGIONAL, THE FEDERAL GOVERNMENT COULD PROVIDE SERVICE IN THE AREAS OF R&D, INFORMATION SHARING AND EDUCATION**

- Sponsor technology transfer and research into rapid detection, investigation and responsiveness to biological, toxic or cyber threats

**THE WATER INDUSTRY CONSIDERED THE AGING INFRASTRUCTURE THE GREATEST THREAT TO THE INDUSTRY. THEREFORE, THE FOLLOW-UP CONCENTRATED ON WAYS TO PAY FOR THE SYSTEM REPAIR AS WELL AS WAYS TO RESPOND TO EMERGENCY ATTACKS OR ACCIDENTS...(CONTINUED)**

- Grant clearances to Industry security personnel so they can access data on Industry threats from Federal sources and develop interchange between security agencies and water industries
- Use trade associations (i.e. American Water Works Association) as a vehicle to educate the public on infrastructure threats as well as sources for information to the government

**THE TELECOMMUNICATION INDUSTRY IS HIGHLY COMPETITIVE AND IS CONCERNED WITH THE PROSPECT OF HAVING TO SHARE VULNERABILITIES AND INTRUSIONS WITH THE GOVERNMENT AND OTHER INDUSTRY PLAYERS**

- Vitesse was not initially convinced that the telecommunications infrastructure is vulnerable to current and foreseeable threats
- Users of telecommunication services are generally aware of a certain level of risks. The telecommunication Industry cannot provide absolute guarantees on system security
- Industry, or their association counterpart, should establish teams which try to invade or disrupt their systems and work with the vendors and customers to reduce the identified vulnerabilities
- Industry remains convinced that they themselves can solve this problem and that they are the most qualified to identify and remedy threats to their own system

**THE TELECOM INDUSTRY IS OPPOSED TO MORE REGULATION AND BELIEVES THAT MUCH HAS BEEN DONE BY THE INDUSTRY TO PROTECT ITS INFRASTRUCTURE. HOWEVER, THE GAME DID DEMONSTRATE POTENTIAL WEAKNESSES AND THE INDUSTRY PROVIDED SEVERAL SUGGESTIONS TOWARD IMPROVEMENT AS WELL AS STATE REQUIREMENTS THAT THEY BELIEVE THE COMMISSION MUST MEET TO ENSURE COOPERATION AND IMPROVEMENT IN INFORMATION SHARING**

- Industry and their association counterparts should establish teams which try to invade or disrupt their systems, then work with the vendors and customers to reduce the identified vulnerabilities
- Allow industries to improve their own security but allow them to recoup the costs of increased security from the government via State or Federal agencies such as the Federal Communications Commission (FCC)
- Government should consider research in technological issues such as unbundling and co-location difficulties
- Liability issues
  - Users must be part of the liability negotiations
  - Other industries must report intrusions - currently few do
  - Federal agencies must pursue and prosecute violators

**THE TELECOM INDUSTRY IS OPPOSED TO MORE GOVERNMENT AND BELIEVES THAT MUCH HAS BEEN DONE BY THE INDUSTRY TO PROTECT ITS INFRASTRUCTURE. HOWEVER, THE GAME DID DEMONSTRATE POTENTIAL WEAKNESSES AND THE INDUSTRY PROVIDED SEVERAL SUGGESTIONS TOWARD IMPROVEMENT AS WELL AS STATE REQUIREMENTS THAT THEY BELIEVE THE COMMISSION MUST MEET TO ENSURE COOPERATION AND IMPROVEMENT IN INFORMATION SHARING (CONTINUED)**

- Any government agency dealing with information sharing and regulation must consider the following issues:
  - Incorporate existing studies in their vulnerability estimates (i.e., SS-7, a standard that defines the procedures and protocol by which network elements in the public switched telephone network (PSTN) exchange information over a digital signaling network to effect wireless (cellular) and wireline call setup, routing and control)
  - Government and Industry must conduct credible analyses of the vulnerability and threat which includes types of threats, methods of prevention and costs of providing security
  - The system must have mechanisms for feedback that protect Industry proprietary information

**THE HEALTHCARE INDUSTRY HAS HAD INCREASING DIFFICULTY IN PROVIDING SECURITY MEASURES TO THEIR CUSTOMERS BECAUSE THEY HAVE BEEN CONSTRAINED BY RECENT FEDERAL GOVERNMENT ACTIONS**

- Projected costs of the increased security needs are at odds with mandated cuts in medical spending
  - Cuts to Medicare/Medicaid have only decreased the ability for healthcare providers to increase their system security
  - The “Healthy Society” concept, with preventive care is more efficient but harder to protect because of its centralization
  
- Efforts to make patient care effective and efficient and increase dependency on other industries
  - Increased reliance on Telecommunications
  - Growing dependency on electronic patient record and pharmaceutical systems
  - Network downtime would cause a substantial loss of revenue, and impact public confidence

**PIONEER PROVIDED A SERIES OF SUGGESTIONS TO THE FEDERAL GOVERNMENT TO ASSIST THEM IN HANDLING THE THREAT**

- An alternative to superagency could be the establishment of a multi-Industry committee to solve Industry problems
  
- Government would become responsible for the following areas:
  - Incentives – provide tax incentives and equipment write-offs for industries who improve infrastructure security
  - Punitive Damages – make punishment for attacks (cyber and physical) severe enough to deter
  - Share information in a timely manner
    - .. Long term threats to be provided periodically
    - .. Make access to information easy to obtain without creating security risks
  - Protect the medical Industry from risk management costs not of its own making
  - Provide quick response to emergencies and improve preparation to coordinate with industries and state and local governments

**THE MEDICAL INDUSTRY AGREED WITH THE COMMON CONCERNS AND SOLUTIONS, THE POST GAME INTERVIEW STRESSED THE ISSUES OF LIABILITY AND DETERRENCE, METHODS OF IMPROVING SECURITY AND EDUCATION**

- Protect the medical Industry from risk management costs not of its own making
- Make punishment for cyber and physical attacks severe enough to deter threats
- Remove technical disincentives like overseas security export controls
- Create an inexpensive and easy reporting mechanism for Industry to retrieve information
- Work with other agencies to improve strong cryptography and strong operating systems
- Provide tax incentives to support funding for security

**THE MEDICAL INDUSTRY SEES A PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC) MODEL AS BEST FOR ANY NEW TYPE OF INTER INDUSTRY/GOVERNMENT AGENCY BUT STRESSED THE NEED TO INCLUDE SMALL AS WELL AS LARGE BUSINESSES**

**THE TRANSPORTATION TEAM CONCENTRATED ON METHODS OF COMMUNICATION BETWEEN GOVERNMENT AND INDUSTRY IN RELATION TO INFORMATION SHARING AND REGULATION. WHILE THEY DID NOT NECESSARILY SUPPORT MORE REGULATION, THEY THOUGHT AN ENTITY SHOULD BE FORMED TO SHARE INFORMATION AND IDEAS**

- The National Security Agency (NSA) was considered the key agency for information sharing
- Small business must be involved, through associations, which they already belong to, in the formation of policy
- The Commission drafts should go to Industry to ensure that the plan is feasible and can be implemented effectively
- Government should institute a tax incentive linked to Industry performance in the field of infrastructure protection

**THE INDUSTRY SUPPORTS DEREGULATION AS A WHOLE BUT REALIZES THAT THREATS EXIST AND THAT AN ORGANIZATION MUST EXIST TO PROVIDE SECURITY ISSUES**

## **THE ENERGY INDUSTRY'S CURRENT SAFETY AND SECURITY REQUIREMENTS PROVIDE FOR THE PROTECTION OF ITS INFRASTRUCTURE**

- To protect U.S. interests, the energy Industry needs to develop its own position in conjunction with Government to facilitate:
  - The development of international agreements and in defining jurisdictional responsibilities
- The Industry has already identified its critical infrastructures and developed redundant systems to protect them
- Additional measures, such as government regulation, will not provide an increase in the level of protection
- The largest threat facing the Industry is from an “insider,” a disgruntled employee/former employee with intimate knowledge of the company’s operations
  - In this case, disruptions would be localized
  - Organized crime is perceived to be more of a threat than foreign terrorism
- The power Industry will continue to conduct self-assessments to identify vulnerabilities
- There is a need to identify and address cross-Industry vulnerabilities and liability issues
- The power Industry is more concerned with state and local government assistance in infrastructure protection and would consider federal involvement only as a final step

**THE ENERGY INDUSTRY REQUIRES LIMITED GOVERNMENT INVOLVEMENT, AND NO ADDITIONAL GOVERNMENT REGULATION, FOR THE PROTECTION OF ITS INFRASTRUCTURE**

- The energy Industry regulatory agency, the North American Electric Reliability Council (NERC), currently has policies regarding the protection of the Industry's infrastructure
  - However, not all producers are part of NERC, and NERC cannot enforce compliance with its policies
  - The market system will drive the Industry to acceptable standards and levels of protection
  
- The Industry will evaluate if “cyber” threats will require additional information, security or funding for research and development
  - A partnership with Government will ensure that the information is broader and more cohesive
  - Industry traditionally has relied on private agencies to perform security analyses on its systems

**THE POWER INDUSTRY ALSO QUESTIONED THE NEED FOR MORE REGULATION AS THEY CURRENTLY ARE HEAVILY REGULATED. THEIR COMMENTS STRESSED THIS FACT**

- The growing globalization of the Power Industry makes it difficult to protect the Industry
  - A US plant exists in Argentina
  - A US plant provides power for 2 million people in the United Kingdom
  - Power is easy to transfer, if a problem occurs in one place, it is easy to get power from somewhere else. However, the integrity of the power distribution grids will be more important as deregulation takes effect

**THE POWER INDUSTRY'S MAIN CONCERN WAS THE LACK OF INFORMATION SHARING BETWEEN DIFFERENT AGENCIES AND INTERDEPENDENT INDUSTRIES. AN ORGANIZATION WOULD BE USEFUL IF IT PROVIDED THIS AS WELL AS GLOBAL INFORMATION WHICH COULD AFFECT POWER INDUSTRIES OUTSIDE OF THE NERC SPHERE OF INFLUENCE**

**THE KLEINGELD TEAM FEELS THAT THE BANKING AND FINANCIAL SERVICES INDUSTRY IS CURRENTLY TAKING THE STEPS NECESSARY TO SECURE THEIR INFRASTRUCTURE**

- The banking and finance Industry has a history of conservatism and risk management which has resulted in a robust operational environment for today's threats and vulnerabilities
  - The Industry has a “security first” philosophy and is very conscious about managing market perceptions
  - Initially, the team did not like the concept of “non-market driven” recommendations because they felt that the Industry would make any investments necessary once they understood the risk
  
- The Industry would oppose additional regulations and/or mandated reporting requirements
  - Industry feels that they are already reporting threat and intrusion data back to the government through the Suspicious Activities Report (SAR) and receives little from the government in return

**THE TEAM RECOGNIZED THE NEW CHANGING ROLE OF THE NATIONAL INFRASTRUCTURE AND BELIEVED THAT WHILE INDUSTRY SHOULD HAVE THE LEADERSHIP ROLE IN INFRASTRUCTURE SECURITY GOVERNMENT SHOULD PARTICIPATE**

- The team believed strongly that government should aggressively pursue computer criminals and recommended improving/enhancing the ability of law enforcement to pursue and prosecute computer criminals
  - The team cited their inability to collect accurate background data on prospective employees from previous employers for fear of breach of privacy issues
  - Government regulatory requirements should include all financial services institutions and their service providers
  - The team clearly believed that government had a significant role in infrastructure protection/mitigation once events reached the nation-state level i.e. structured physical/cyber attacks against the national infrastructure
  - The team was not opposed to penalties for Industry players who fail to meet certain minimum security standards

**THE BANKING INDUSTRY WANTS A THREE-PRONGED STRATEGY TO PROTECT THE BANKING INFRASTRUCTURE. THEY INCLUDE:**

- Preventive protection:
  - An improved Demand Deposit Account - these are the monies that are at the core of the banking system - it is the funds that are on deposit with a financial institution, typically in a checking or savings account, and have access to "on demand" i.e. a check, going to a teller or an ATM
  - A better Account Information Security system
  - A method by which National Security Agency (NSA) shares its encryption capabilities
  - Expand the role of NSA in penetration testing in key infrastructures
- Improve detection
  - Determine better ways to insert software code to find flaws in the system
- Stronger reaction
  - Improve the response time between an attack and notification to the appropriate law enforcement and regulatory agency

**THE BANKING INDUSTRY, LIKE OTHER INDUSTRIES, STRESSED THE NEED FOR INFORMATION SHARING, INDUSTRY STANDARDS AND OPERATIONAL CONTROL WITH GOVERNMENT PROVIDING INFORMATION AND FUNDING. HOWEVER, THEY HAD SPECIFIC OBJECTIVES IN MIND WHICH DIFFER SOMEWHAT FROM OTHER INDUSTRIES. THEY REQUESTED ACCESS TO GOVERNMENT CAPABILITIES TO IMPROVE THEIR OWN SYSTEM AND ENSURE ACTION FROM EXISTING GOVERNMENT AGENCIES RATHER THAN CREATING A NEW REGULATORY AGENCY**

**INDUSTRY IS CURRENTLY FACED WITH PROTECTING THEIR OWN INFRASTRUCTURE OR ACCEPTING GOVERNMENT REGULATIONS AIMED AT MANDATING PROTECTIVE MEASURES. BOTH OPTIONS HAVE INDUSTRY CONCERNED**

- If the government wants a higher level of protection, companies expect the government to provide incentives, regulatory relief or loan guarantees to facilitate this process
- The early threats (levels one and two) were easily managed because of investments already made to prevent or mitigate effects of threat, or that it was an acceptable risk or cost of doing business
- Possible loss of revenue due to loss in public confidence was a greater concern and had more significant potential impacts than spending additional funds to correct a weakness or problem
- With physical threats, confidence in and reliance on law enforcement's ability to prevent or reduce attacks, limit investment in physical protection and security. (Why pay for a second police force?)
  - Confidence in law enforcement is not as great against cyber threats, therefore requires additional investment
- Only when risk is clearly quantified can companies estimate the potential cost, and quantify the benefits of preventing the impact of a threat
  - Industry teams did not feel that threats were adequately defined and therefore expenditures or capital outlays could not be assessed

**INDUSTRY IS CURRENTLY FACED WITH PROTECTING THEIR OWN INFRASTRUCTURE OR ACCEPTING GOVERNMENT REGULATIONS AIMED AT MANDATING PROTECTIVE MEASURES. BOTH OPTIONS HAVE INDUSTRY CONCERNED (CONTINUED)**

- The economic impact of threats to utilities (power, gas, water) is not as great because of their monopoly position and inelasticity of demand
- Liability issues change companies' outlooks on impact of threats
  - Insurance coverage limits company's capital outlays to recover from an event
  - Outsourcing reduces the direct impact to companies by shifting the liability to third parties

Government Team Insights ...

**THE GOVERNMENT TEAMS WERE ASKED TO ASSESS PCCIP RECOMMENDATIONS, MAKE SUGGESTIONS TO CHANGE THEM AND ULTIMATELY PROVIDE ALTERNATIVES**

- The Executive team initially used the recommendations to draft policy, identify Government responsibilities and recommend legislative programs
- The Congressional team identified key issues that the federal government should act on to enhance critical infrastructure protection and take into account the concerns of Industry, state and local governments
- The State and Local team assessed the impact of the PCCIP “strawman” recommendations on their constituents, make changes and provide alternatives according to their needs
- In Move 2, all Government teams were tasked to assess the effectiveness and viability of the program they produced in a changed environment of new threats

**BASED ON THE PCCIP “STRAWMAN” RECOMMENDATIONS, THE EXECUTIVE TEAM DEVELOPED A POLICY (S.99, A FICTITIOUS BILL) TO ENHANCE INFRASTRUCTURE PROTECTION WHICH CAUSED A STRONG INITIAL RESPONSE FROM BOTH CONGRESS AND SEVERAL INDUSTRY TEAMS CONCERNING THE NEED FOR CERTAIN ASPECTS TO BE INCLUDED IN THE PROGRAM**

- The policy/program, proposed the creation of a super-agency, for infrastructure protection based on the premises that:
  - Existing federal processes are inadequate to address critical infrastructure protection
  - Standards, procedures, research, and technology programs associated with critical infrastructure protection are inadequate to meet likely future threats
  - The level of awareness about the need for critical infrastructure protection is inadequate in Industry and the nation as a whole
- Industry and Congress felt a new federal agency was not needed, but rather a reorganization of existing federal resources and assignment of coordinated responsibilities
- A mechanism is needed for intelligence and law enforcement communities to collect and disseminate information on threats and vulnerabilities to the appropriate groups
  - Appropriate communication with the private sector must be ensured
  - National consciousness and risk awareness must be raised
  - Formal training must be provided through higher education
  - Establishment of a central information clearinghouse
  - Will require change in laws, policy and regulations because of current limits on intelligence and law enforcement activities

## **THE FINAL RECOMMENDATIONS OF THE EXECUTIVE TEAM PROVIDED DIRECTION FOR THE COMMISSION TO INCORPORATE INDUSTRY CONCERNS WITH GOVERNMENT RESPONSIBILITIES**

- The Federal role is to coordinate/orchestrate regional efforts into a seamless national “Infrastructure Safety Net” by building on existing relationships
  - Encourage Regional, State & Local and business alliances to raise awareness and promote information sharing
  - Ensure that sector-specific solutions and processes are coordinated
  - Determine how stakeholders are responding through existing relationships
- Government should rely primarily on market forces for infrastructure development and growth
  - Initial reliance on market-based strategies
  - Incentive based programs are necessary where shortfalls exist
- Education, training and awareness programs must be developed for critical infrastructure protection

## **THE STOVEPIPING OF COMMUNICATION AND INFORMATION WITHIN THE FEDERAL GOVERNMENT WAS A FUNDAMENTAL CONCERN IDENTIFIED BY THE INDUSTRY TEAMS**

- The Government must rely on market forces as the principal driver for infrastructure protection investments
  - Competitive and economic pressures currently drive secure and reliable systems
  - Infrastructures have been hardened by experience
  
- Extensive reporting requirements already exist; however
  - Redundancy exists between multiple government agencies
  - Data is not coherently collected, analyzed, and distributed
  - Feedback mechanisms are inadequate
  
- Cultural and legal impediments prevent the sharing of information between the intelligence and law enforcement communities

## **THE CONGRESSIONAL TEAM ALSO RECOGNIZES THAT INDUSTRY MUST PLAY THE PRIMARY ROLE IN PROTECTING ITS ASSETS**

- Education and awareness programs will significantly enhance infrastructure protection
  - Needed at all levels of Industry, including CEO level
  - Undergraduate and graduate level programs
- A mechanism must be developed that will gain the confidence of the private sector so that intrusion information can be shared with and protected by the federal government and threat information can be responsibly disseminated to the private sector
- The Federal Government should designate a focal point to act as a nexus for federal agencies and the private sector to share critical information. This focal point should be:
  - Adequately funded
  - Assigned specific responsibilities
  - Held accountable
- However, where the Government identifies shortfalls, incentives are appropriate to stimulate further investment and enhancement of the critical infrastructure assets

## **THE STATE AND LOCAL TEAM MAINTAINED A CLEAR CONCISE MESSAGE TO THE PCCIP CONCERNING THEIR RECOMMENDATIONS**

- Education should be the number one goal for the federal Government in order to gain public and private acceptance of new measures
- It is imperative that government gain the trust of Industry by providing them with all of the information, “not just parts of it”
  - This can be done by creating a joint Industry/Government advisory council to develop a clearinghouse for reporting confidential infrastructure breaches and to analyze and share threat assessments. The joint council would also advise Industry on the development of standards and monitor Industry efforts in this area
    - .. Provide a team approach, or “partnership” as opposed to Government mandating new regulations on business
    - .. Does not create additional bureaucracy merely improves coordination with existing entities
    - .. Provides more aggressive technology transfer in research and development
- We must not create additional bureaucracy
  - A superagency will impose a tremendous cost on state and local Governments in addition to providing Industry standards that will force many small businesses out of business
  - State and Local Government must be involved from the start in order to represent their constituents
  - Distribution of threat information must be extended to state and local agencies so that they also have the opportunity to react and prepare for future threats

State and Local Team Insights ...

**THE STATE AND LOCAL TEAM MAINTAINED A CLEAR CONCISE MESSAGE TO THE PCCIP CONCERNING THEIR RECOMMENDATIONS... (CONTINUED)**

- With the right training and information the state can provide technical expertise to respond to the cyber threat
- FEMA and the state and local agencies already exist to respond to emergency crisis situations

Simulation Observations ...

**THE SIMULATION PROMOTED IMPROVED AWARENESS IN THE FOLLOWING KEY AREAS:**

- Threats to the infrastructure
- The role of government in protecting the infrastructure
- Industry initiatives and ideas
- Costs and burdens associated with infrastructure protection
- Obstacles to the implementation of Commission recommendations
- Interrelationships/Interdependencies between infrastructures

Simulation Observations ...

## **THREATS TO THE INFRASTRUCTURE**

- Vulnerabilities:
  - The growing dependence of the critical infrastructure on information technology is creating new vulnerabilities
  - The extent of current and future threats are not fully recognized
  - Industry invests in security and protective mechanism to meet existing threats, but does not have the information to reduce vulnerabilities to future threats

## **THE ROLE OF THE GOVERNMENT IN PROTECTING THE INFRASTRUCTURE**

- Industry is clearly concerned over increasing the burden of legislation and mandates to the infrastructure
- The state and local governments establish the criteria for safeguards against the threats and emergency response in the aftermath of an attack
- Industry recognized the need for more information from the federal government regarding the threats. They believe the government should
  - Provide “real time” intelligence on imminent threats to specific segments of the infrastructure
  - Forecast long term threats so that Industry can develop protective mechanisms
- Government should provide increased funding in the following areas
  - Provide money for R&D for security needs
  - Increase education and awareness of the threats to the infrastructure
- Law enforcement and intelligence agencies should increase their focus on cyber threats
- Existing Government Agencies and organizations should be integrated to address the issue of the cyber threat
  - A process for effective information sharing and protective technology

## **INDUSTRY INITIATIVES AND IDEAS**

- Industry and government must partner to combat the threat to the infrastructure. Industry has suggested forming the National Infrastructure Coordination Council (NICC), a private Industry led consortium which shares information among Industry and with government
  
- The NICC would also utilize methods which allows Industry to share infrastructure protection
  - Should be a voluntary effort, based upon existing association memberships
  - Should be based out of the White House
  - Needs of small business must be represented
  
- Market competitiveness is an effective tool to motivate individual companies to safeguard themselves against current cyber, or physical threats
  
- Trade organizations and Industry associations should be utilized to provide Industry trends and or vulnerabilities to the government and should serve as the basis for disseminating government threat information
  
- Industry can provide the necessary safeguards against a viable threat. Incentives must be developed for Industry to make the necessary investments to infrastructure protection when a threat is not clearly identified

## **COSTS AND BURDENS ASSOCIATED WITH INFRASTRUCTURE PROTECTION**

- Both the government and private Industry are concerned with the costs associated with effectively protecting the infrastructure
  - State and local governments are concerned with unfunded mandates on Infrastructure Protection being legislated from Washington
  - Congress is reluctant to expand the role and nature of government
  - Government agencies are also restricted by budget reductions
  
- Government mandates for increased private funding of infrastructure protection may force companies out of state or offshore

Next Steps ...

## **ISSUES FOR CONSIDERATION**

- Recommendations by the Commission should be specific and include the process for implementation and be shared with Industry
- The Commission should share findings from the simulation with key members of the Department of Defense, Congress, Law Enforcement Agencies as well as the Intelligence community
- A process for increased cooperation and communication between government and the private sector must be developed
- The roles and responsibilities of current government departments and agencies must be specified for dealing with cyber threats and crimes
- Liability and Industry linkages, interdependencies, vulnerabilities and responsibilities must be addressed
- Continuing education on the nature of plausible current and future threats and system vulnerabilities is necessary to build public and Industry support for implementation of the commission's recommendations