President's Commission on Critical Infrastructure Protection

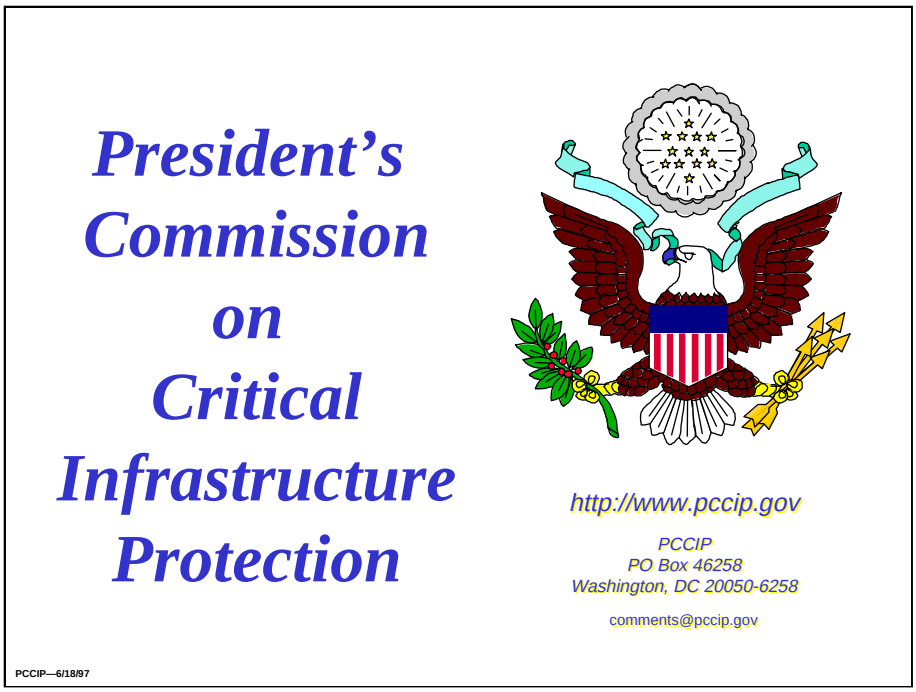
OVERVIEW BRIEFING

June 1997

http://www.pccip.gov

PCCIP
PO Box 46258
Washington, DC 20050-6258

comments@pccip.gov



OVERVIEW BRIEFING

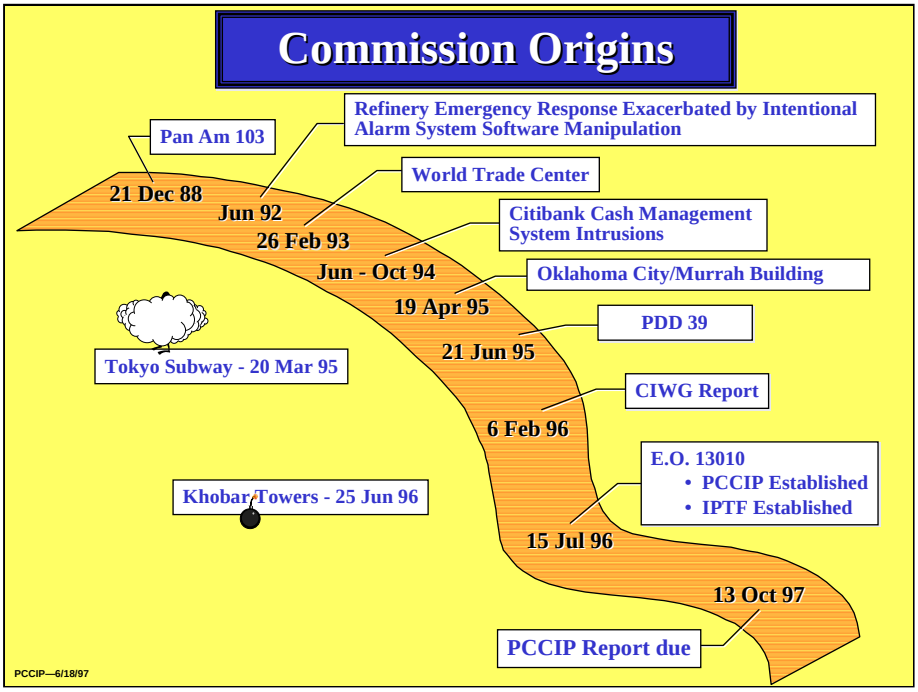
INTRODUCTION

The President's Commission on Critical Infrastructure Protection (PCCIP) was created by Executive Order 13010, signed by the President on July 15, 1996. The Executive Order originally stated that the Commission would terminate after one year; however, the order has since been amended to extend the life of the Commission by three months, to October 13, 1997.

The Commission is therefore well along in its fifteen-month task of assessing physical and cyber threats to our vital infrastructures and developing policies and strategies to protect them. This overview briefing reports on the status of our work to those elements of the public and private sectors that have an interest in infrastructure assurance issues. We invite your participation as our work continues.

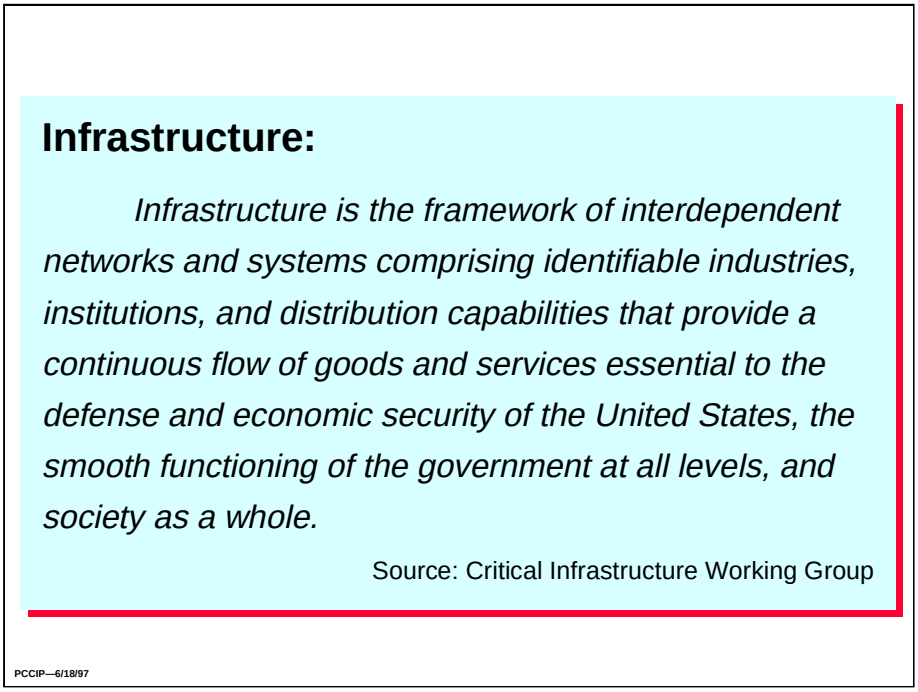
Infrastructure protection is a broad subject of great complexity. At the outset we devised an approach to the task, and as work has progressed we have begun to form some general, preliminary impressions. Our outreach program has been extensive, but there are many knowledgeable sources we have not yet explored, and others yet to be discovered.

We are by no means certain of our final findings and recommendations. What follows is intended to provide a sense of some of the issues we are exploring in the quest to find workable solutions to a serious problem.



Commission Origins

The President's Commission on Critical Infrastructure Protection (PCCIP) traces its origin to a recommendation of the Critical Infrastructure Working Group (CIWG), which was created by the Attorney General in response to Presidential Decision Directive 39 regarding terrorist threats to the United States. The CIWG conducted an intense, but short-term, examination of the threats and vulnerabilities of critical national infrastructures. Its February 6, 1996 report recommended creation of two organizations to address current and future threats and vulnerabilities. For the longer term, the PCCIP was established and charged to conduct a comprehensive review of infrastructure protection issues and recommend a national policy for protecting critical infrastructures and assuring their continued operation. As an interim measure, while the Commission is conducting its analysis and until the President has an opportunity to consider and act on its recommendations, the Infrastructure Protection Task Force (IPTF) was established. The mission of the IPTF is to increase coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that could have a debilitating regional or national impact.



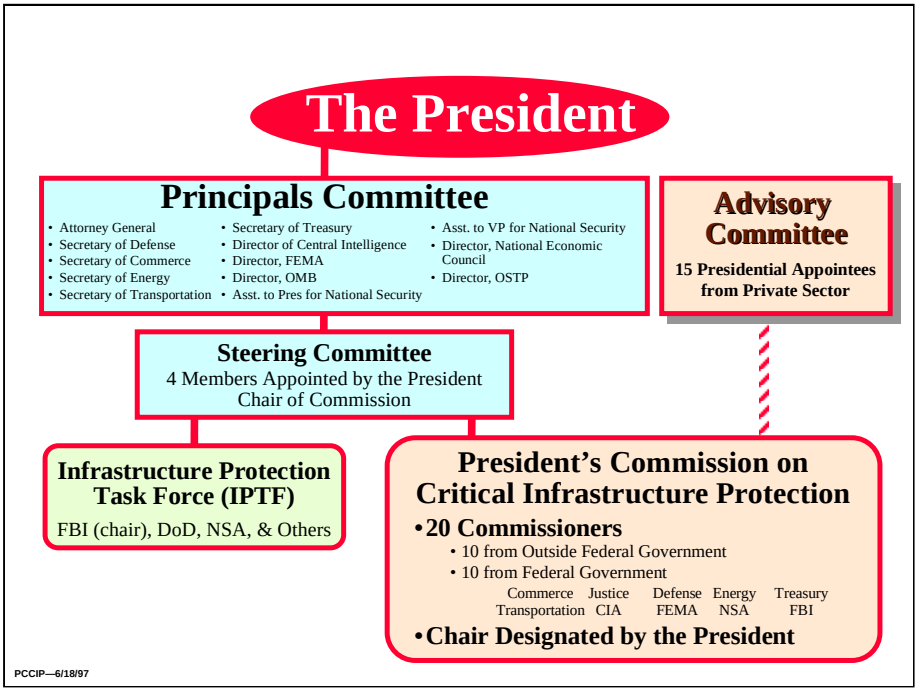
Terms of Reference

The CIWG's report took a first cut at defining "infrastructure" as seen here. Executive Order 13010 went on to describe "*certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.*" These infrastructures include

- telecommunications
- electrical power
- gas and oil storage and transportation
- banking and finance
- transportation
- water supply
- emergency services (including medical, police, fire and rescue)
- government services.

Threats to these infrastructures include physical threats to tangible property and "cyber threats" — electronic, radio-frequency or computer-based attacks against the information infrastructure or its components.

The Commission is charged with recommending a comprehensive national policy and an implementation strategy for protecting critical infrastructures from both ***physical*** and ***cyber*** threats.



Structure

Executive Order 13010 created a structure for the PCCIP's operation and related activities. The structure depicted exists now, although not all positions have been filled.

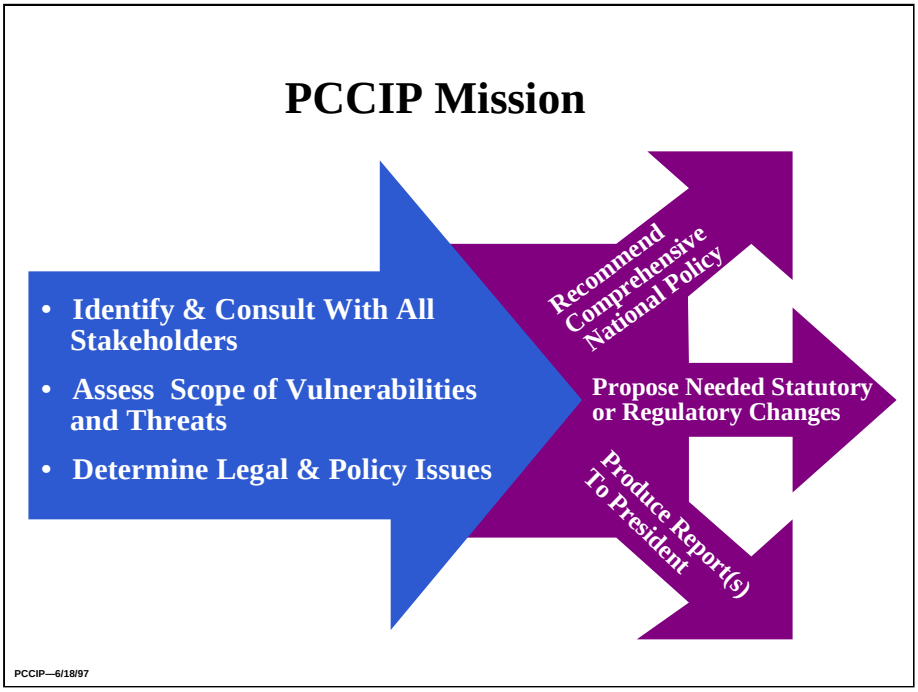
The Principals Committee consists of selected department and agency heads, plus designated officials from the Executive Office of the President.

The Steering Committee, which oversees the work of the Commission on behalf of the Principals Committee, consists of Commission Chairman Tom Marsh and four officials appointed by the President. Current appointees are Sandy Berger, Assistant to the President for National Security Affairs, and John White, Deputy Secretary of Defense.

The Commission itself is drawn from the ten executive branch departments and agencies listed in the Executive Order and shown on the chart above. The head of each agency was directed to nominate not more than two full-time members of the Commission, of which one could be an individual from outside the Federal Government. All ten Federal government Commissioners have been on board since the Commission's inception. Recruitment of private sector experts as Commissioners began immediately, and the first members from outside the Federal government reported for work in February, 1997. In all, seven Commissioners have been appointed from the private sector.

The IPTF is fully operational within the Department of Justice and is performing the interim coordination mission assigned to it by the Executive Order.

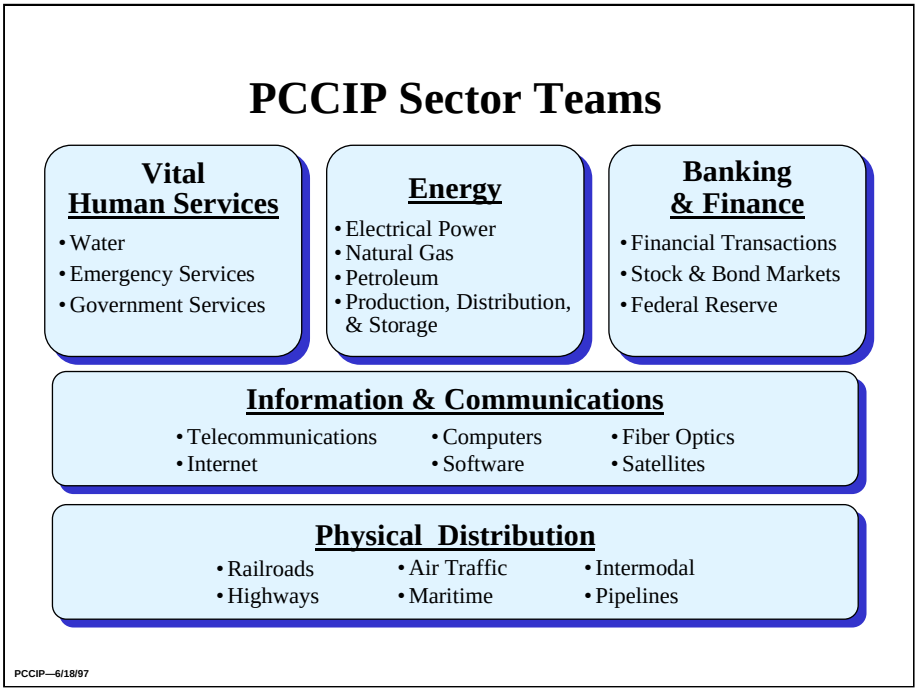
On June 6, 1997 the first five members of the Advisory Committee were announced. Additional appointments are expected soon.



Mission of the Commission

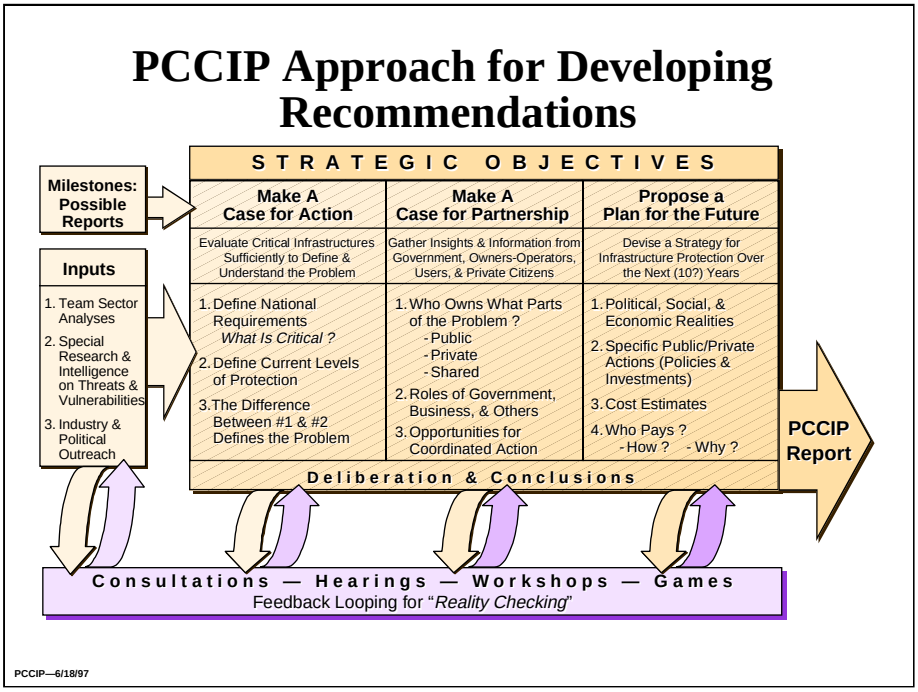
The Commission's mission is to:

- Assess the scope and nature of threats to, and vulnerabilities of, critical infrastructures.
- Determine what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed.
- Recommend a comprehensive national policy and an implementation strategy, including necessary statutory or regulatory changes, for protecting critical infrastructures from physical and cyber threats and assuring their continued operation.



Commission Organization

The Commissioners initially organized into five teams addressing the eight infrastructures as illustrated here. More recently, working groups have been formed to address various "cross-cutting" issues that emerged from the preliminary studies of the sector teams. These issue teams are now working to address a broad range of issues such as public trust and confidence, information sharing, the need for education and awareness, and incentives for infrastructure investment.



Approach

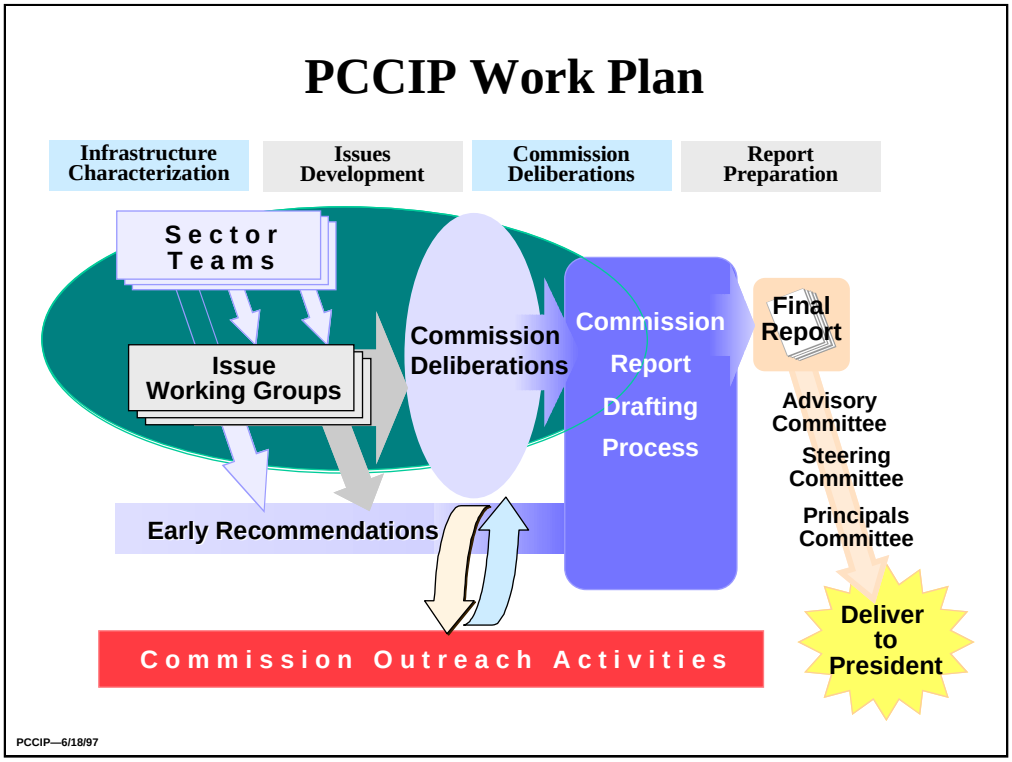
We spent the initial months of our effort evaluating the national infrastructures to understand the nature of our dependency upon them and to identify the vulnerabilities and threats that exist or could exist in the future. Our approach recognizes the fact that most of the infrastructures are privately owned and operated. Any solutions we propose must be viable in both the marketplace and the public policy arena.

Our approach is future-oriented. There is no evidence of an imminent threat of a major attack on our infrastructures, and many operators in the private sector emphasize their past successes in recovering after major natural disasters. However, there is a growing interdependence among infrastructures. And there is a growing use of telecommunications and computer systems for operations, management, and financial exchange.

Almost every group we meet with voices concerns about threats and vulnerabilities. They emphasize the importance of developing approaches to the protection of infrastructures *before* the threats materialize and produce massive system outages. Most of the infrastructures are privately owned and operated within a broad framework of government policy and regulation. Others, just as important to the national economy and security, are owned by the government. Thus, it is increasingly important to assure that the concerns and interests of the public and the private sectors are reflected in responses to infrastructure threats and vulnerabilities. Equally important, the shared nature of infrastructure responsibilities suggests the need for investment by infrastructure owners, operators, and users, as well as by federal, state, and local government.

Commission Consultations

Executive Order 13010 directs us to consult with stakeholders in each infrastructure area—ranging from all levels of government to owners and operators, consumers, and a variety of other interested parties. To accomplish this, we are conducting extensive outreach to collect information, ideas, and opinions for consideration. Included are meetings with individual infrastructure users and providers, as well as the public meetings we have held in Los Angeles, Atlanta, Houston, Boston, and St. Louis. From the outset, we have encouraged the submission of questions and comments by anyone with something to contribute, and we have established our own World-Wide Web site to facilitate such interaction (http://www.pccip.gov/). In addition, we are meeting with labor organizations, trade associations, consumer groups, experts in academia, and government officials at all levels, with several hundred such meetings held to date. Congressional perspectives are being gathered through a series of meetings with committee staffs and interested members of Congress. The Commission is also sponsoring a number of activities, including gaming events and workshops, to provide additional opportunities for focused exploration of assurance-related issues.



Commission Process

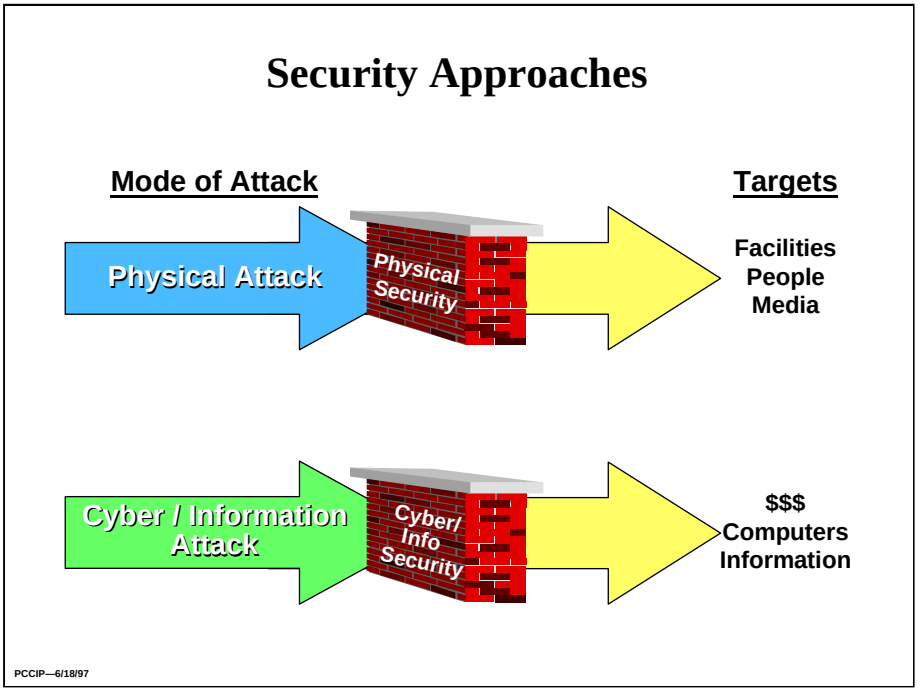
Our work plan is depicted here. Included are periodic reports to the Steering and Advisory Committees to elicit their critical comments and guidance on our efforts. Work underway includes:

Infrastructure Characterization. Our initial research phase sought to "map" each infrastructure and its stakeholders. It identified vulnerabilities and threats, as well as the inter-dependencies among infrastructures, technological problems, needs, and potential solutions. An important objective of this initial step was identification of "cross-cutting" issues—those issues that affect an infrastructure but are either beyond its control or clearly of interest to other infrastructures as well.

Issue Development. In this phase, sector and issue teams have been developing and analyzing the specific issues that emerged from our research phase. This effort is intended to ensure adequate understanding of each issue such that the options for solutions can be related to specific problems—including technological needs, government policies and structures, public-private policies, and others. For each issue, we are developing a range of options that will be thoroughly aired and discussed with all interested parties to ensure that all viewpoints are considered in the Commission's deliberations.

Commission Deliberations. This segment is planned as an intensive process to arrive at conclusions based on the previous analytic work. The Commission will select a specific solution set from among the ranges of options developed in the issue papers. This solution set will form the basis for the Commission's recommended national infrastructure protection policy and implementation strategy.

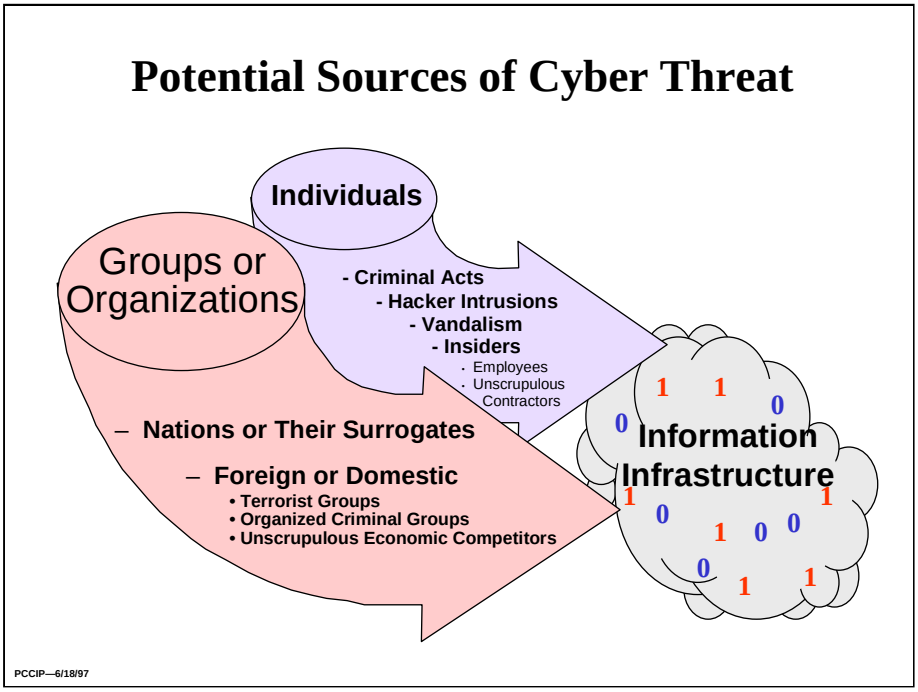
Report Preparation. Writing and vetting the Commission's final report will culminate our work process. We will develop and draft conclusions and recommendations, review them with various advisors to the Commission, and prepare final recommendations for presentation to the President through the Steering and Principals Committees.



Physical Security versus Cyber Security

The government and private sector operators of infrastructures have a long history of dealing with natural disasters and man-made physical threats. However, both sectors are increasingly dependent on telecommunications and computer processing for the management and operation of these infrastructures. The very power of these new technologies opens them to unintended consequences. Cyber threats are real. Groups meeting with the Commission have offered many examples of unauthorized access to proprietary information, fraudulent diversion of funds, and disruption of commercial transactions. Reliance on the Internet and public switched networks creates a new vulnerability of infrastructure operating systems to penetrations and unauthorized access.

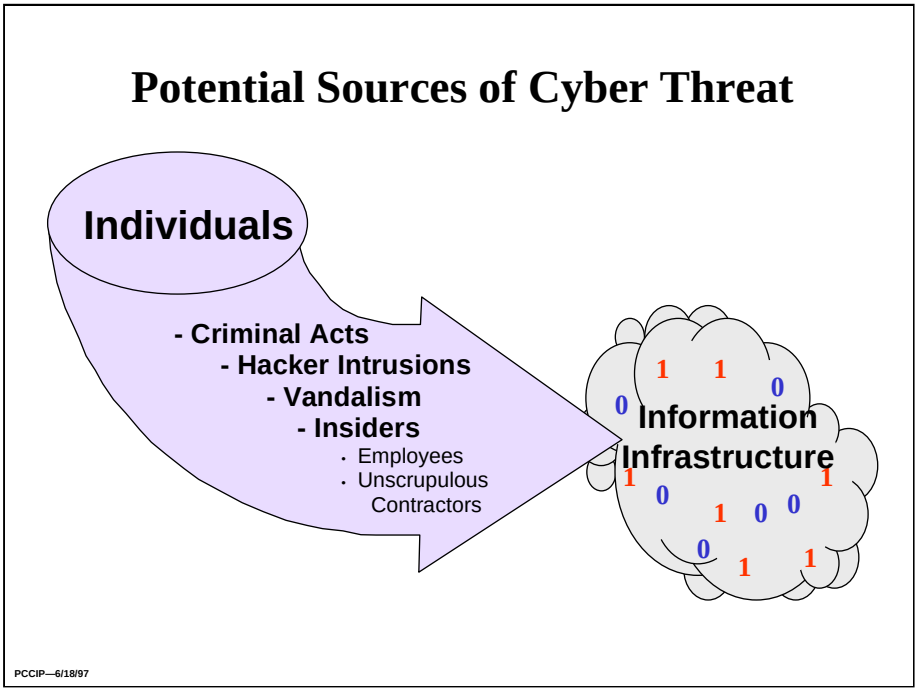
Recent cases of electric power and telephone outages have not been so severe as to compromise the nation's economy or its security. But, while not *currently* at a critical stage, the assurance of critical infrastructures will be increasingly at risk if emerging cyber security and countermeasures needs are not addressed.



Sources of Cyber Threat

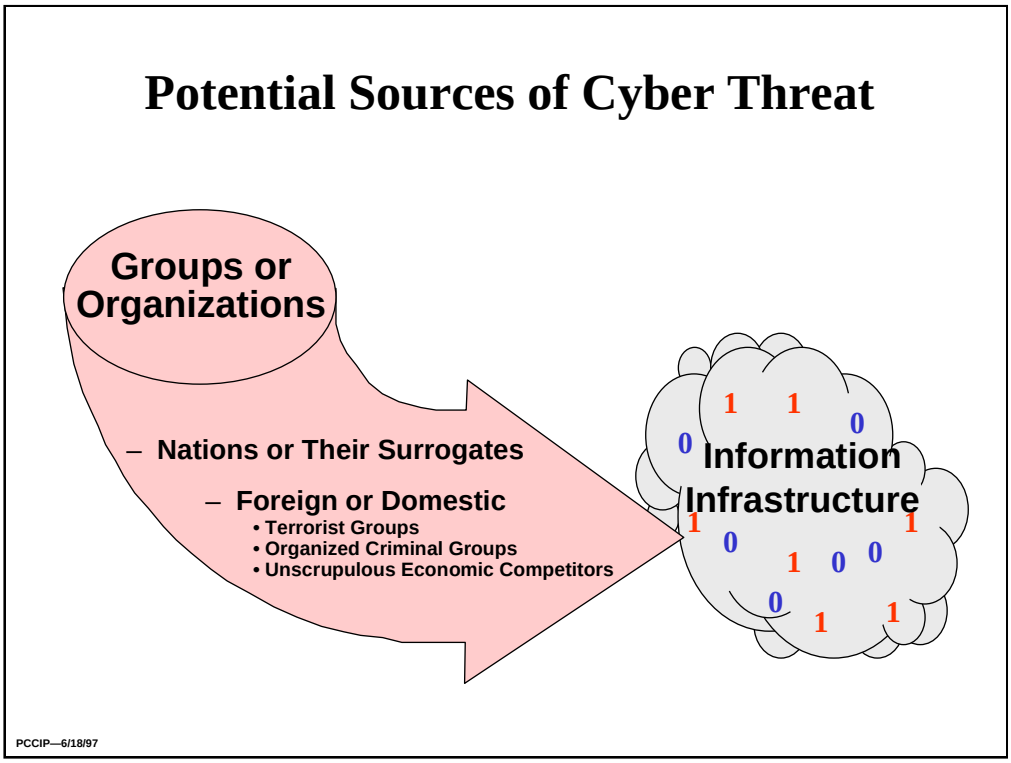
While physical threats are serious, cyber threats which undermine national economic viability are equally important. These threats take on a more serious nature with the growth of the global economy. Few major companies operate without dependency on foreign sources for materials, products, or markets. Just-in-time delivery of products requires transportation tracking and reporting systems. The requirement for rapid financial settlement creates an enormous flow of economic information by cyber means.

Potential threats in the cyber dimension come from individuals and from groups or organizations.



Threats from Individuals

Threats posed by individuals range from simple mistakes by operators, to intentional damage by disgruntled employees or malicious intrusions by hackers, to deliberate theft or fraud by criminals. Cyber-extortion schemes resembling "protection rackets" in which "insurance" is paid to preclude damage have received some notoriety in the media, but our research has found limited evidence of such activity. Today, *insider* crime represents the largest category of cyber attacks in the United States. Tomorrow, insider crime may pale in comparison to organized threats.



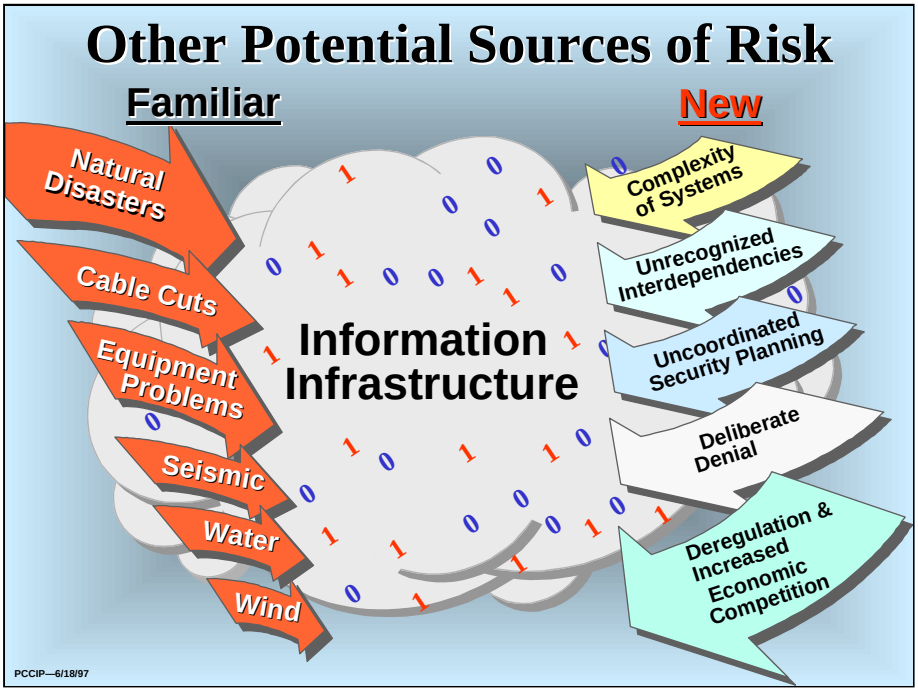
Threats from Nations, Groups, or Organizations

Physical and cyber threats to US infrastructures are considered to have greater potential for damage when they come from groups or organizations than from individuals. The bombings of the World Trade Center in New York, the Federal Building in Oklahoma City, and the Khobar Towers in Saudi Arabia indicate how destructive the work of even small organized groups can be.

Organized criminal groups in the United States appear to be concentrating on transactional crime rather than infrastructure disruption. Evidence of such transactional crimes is generally anecdotal. We believe the sparsity of specific information is due more to the reluctance of members of the financial community to discuss their cyber security problems than to an absence of such problems.

Based upon our consultations with industry, it appears that threats from unscrupulous economic competitors are of concern throughout the US business community. Industrial or economic espionage—targeted against proprietary information—is a major concern. Design, pricing, marketing, bid strategy and similar data have already been compromised using cyber tools. Resulting damage to companies and the nation's global competitiveness can be significant. Physical security, personnel security, information security, cyber security and document security all play a role in coping with this threat.

Given what we know about the means available for attacking US infrastructures in both the physical and cyber dimensions, our concern is that such means could be acquired and employed by a nation-state or terrorist organization intent on doing harm to our country and our way of life.

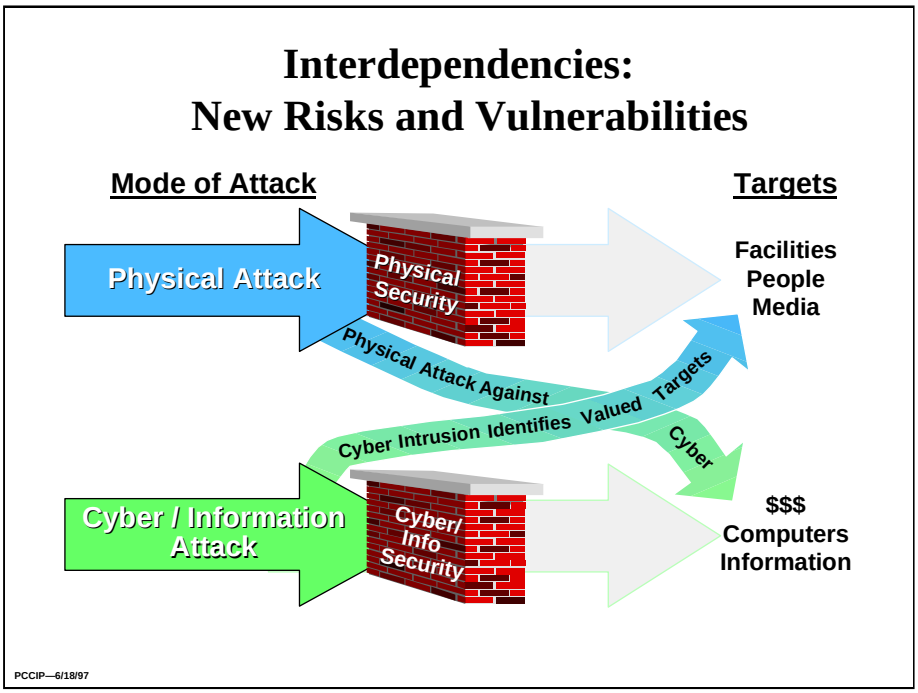


Other Potential Sources of Risk

The Commission's charge is not limited to investigating known threats to existing infrastructures. It also extends to new risks that may emerge from increasing reliance on the information infrastructure throughout our economy and society.

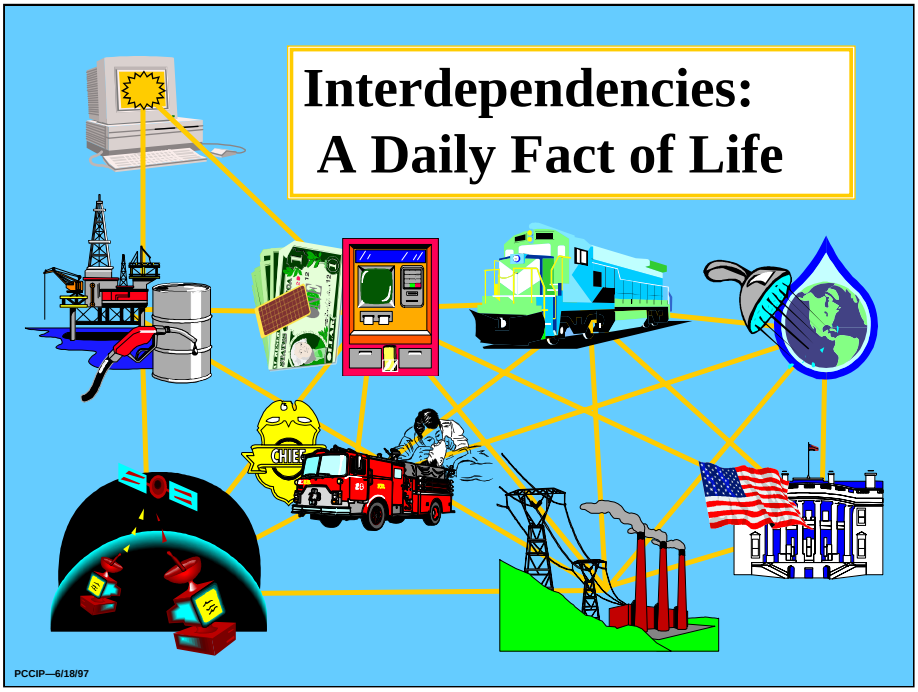
In reviewing plans for response to threats, most infrastructure managers take for granted that all other infrastructures are going to be there when needed. The fuel supplier will refill the tanks of the emergency power generation system. The cooling water will be there when needed to keep the computers running. But interdependence creates new vulnerabilities, and the Commission is proceeding with the objective of minimizing risk of simultaneous failure.

What we have learned to date suggests that these dependencies among infrastructures reflect new risk profiles and require new concepts for security planning. The complexity of systems—due largely to increased reliance on the speed, efficiency, and reliability of information and computer systems for control functions—raises the possibility that an individual infrastructure may not recognize all aspects of its own dependence on other infrastructures.



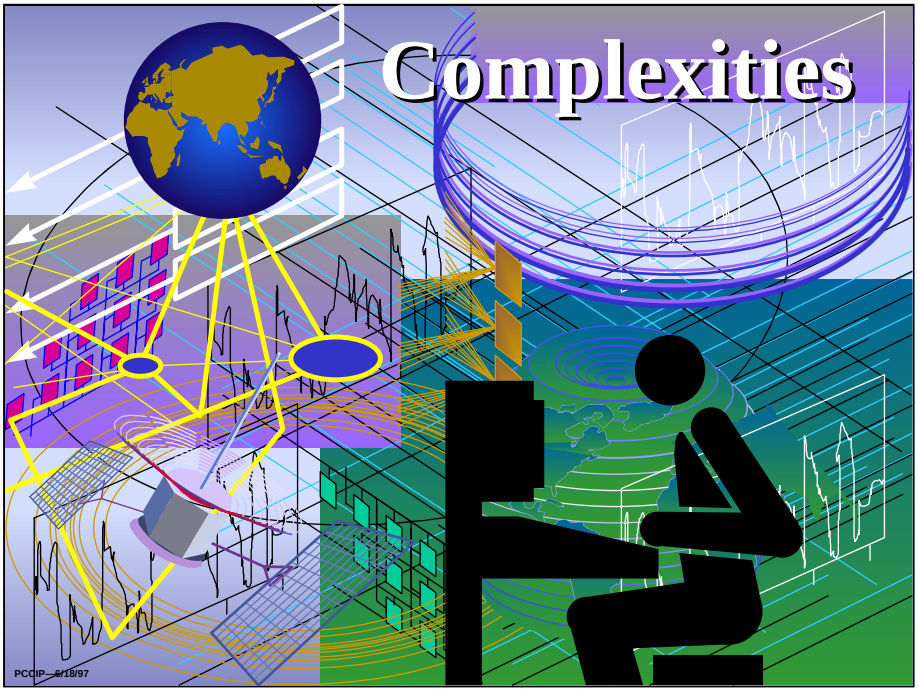
Interdependencies

An example of a new risk is the little recognized but increasing interdependency between cyber and physical systems that may create vulnerabilities in both. Physical and cyber security must be examined in the context of this relationship to appreciate the overall potential vulnerability of an infrastructure. Each system, seemingly secure in its own right, may be affected by an attack. Better coordination is needed between the disciplines of physical and cyber security planning. In the wrong hands, cyber capabilities add a new dimension to physical attacks. They provide new means for gathering and analyzing critical information, with reduced likelihood of detection, that can identify critical nodes and single points of failure. Finally, cyber systems themselves, or their critical links and nodes, could also be targets for physical attack.



Interdependencies

The issue of interdependence deserves special consideration. Businesses in the United States are successful in large part because the infrastructures work. When the switch is flipped, the lights come on. When the spigot is turned, potable water flows. The mail comes in a timely way. Our infrastructures permit low cost, extensive air travel and transport. Private delivery companies are able to guarantee on-time performance because of the existence of highly effective infrastructures. And the new infrastructure element, the Internet, now serves us all in remarkable new ways.

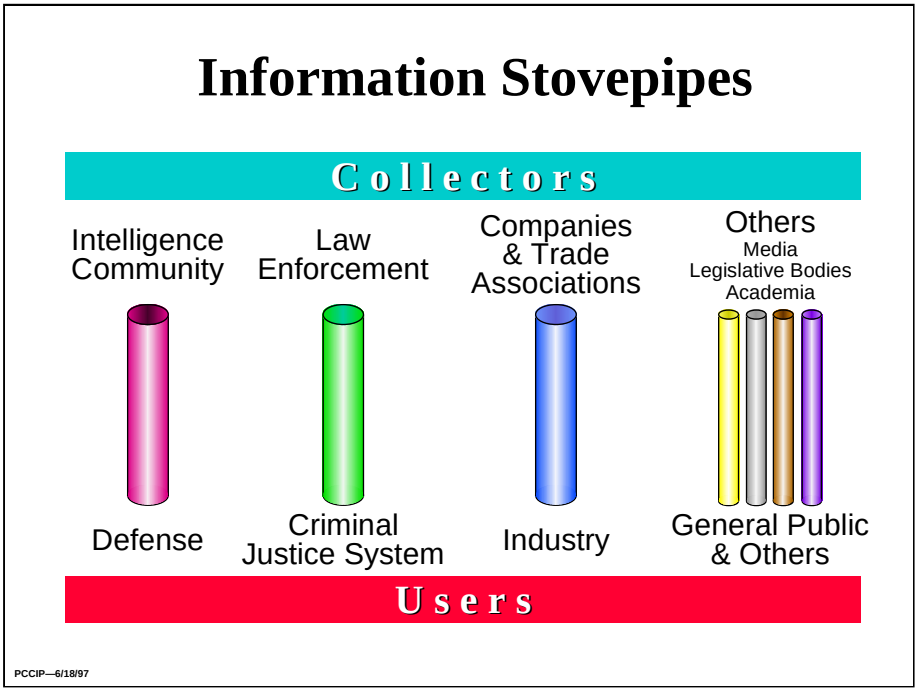


Complexities

The complexity of automated systems induces additional risk. Management awareness and operator training may lag hardware or software upgrades, increasing error-induced accidents. Aging legacy systems—pushed beyond design margins or held together by undocumented software patches—may fail and precipitate serious infrastructure failures. When these or other factors combine, individual failures can trigger more failures, producing a cascade of damage within an infrastructure and possibly other infrastructures. The competitive pressure on key infrastructures resulting from deregulation may generate additional vulnerabilities as system capacity is pared. Less reserve capacity and less system redundancy make infrastructures more fragile. In times of stress, such as during reconstitution from an earthquake, the consequence of such draw-down may prove far more costly than the earlier savings. In the case of energy, for example, draw-down savings must be balanced against potential losses to users during outages, such as damage to stock, lost production, lost sales, and lost wages. Today's risk profiles may be outmoded.

Threats, Risks, and Motivations

In summary, infrastructures are exposed to risks from diverse causes. Threats, risks, and motivations represented above imperil the national information environment which increasingly underpins the physical elements of our national infrastructure. Exacerbating this problem is the fact that our government and society are structured in a way that inhibits sharing of information essential to countering these emerging risks.

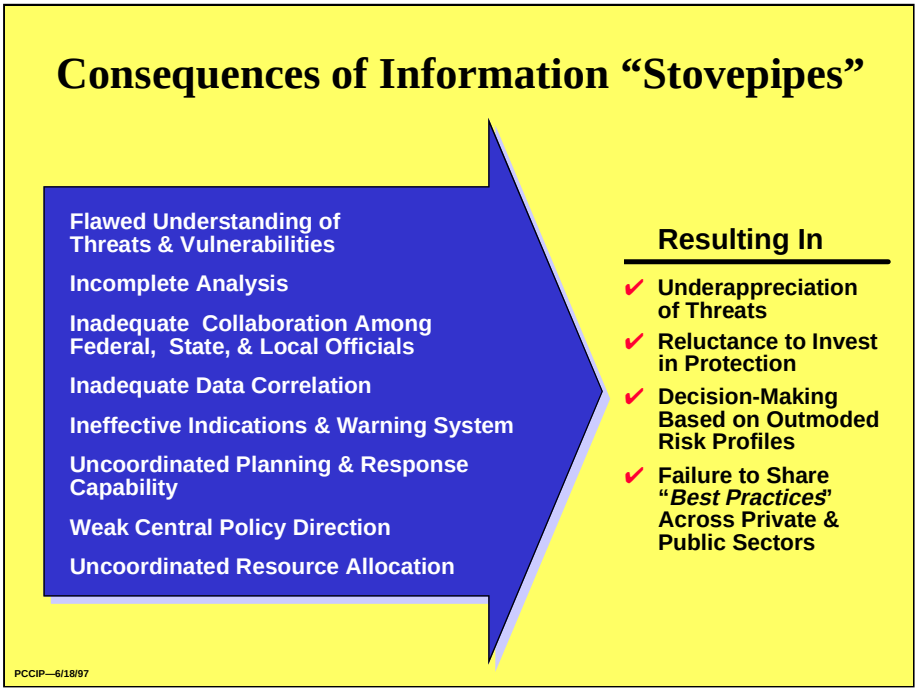


Jurisdictional, Legal, and Private "Stovepipes"

For important reasons, the authority of individual government departments and agencies to collect and disseminate information has been carefully circumscribed—by statute, executive order, or regulation. These carefully defined authorities that pertain to a particular community or industry can act as "stovepipes," permitting information about emerging threats and actual penetrations or attacks to flow up and down within narrowly defined channels but preventing it from flowing across to those in other infrastructures or communities who need to know. National security concerns, for example, prevent widespread dissemination of information about infrastructure threats when such information has been gathered from sources whose identity must be protected.

The private sector finds the free flow of information similarly restricted. The resources required to collect information may be too great for an individual company. And business executives feel that release of information about attacks, especially successful attacks, may subject them to stockholder suits and loss of customer confidence.

Accordingly, the government is constrained by security issues from advising the private sector regarding threats, and the private sector is constrained by commercial concerns from talking to the government about attacks.

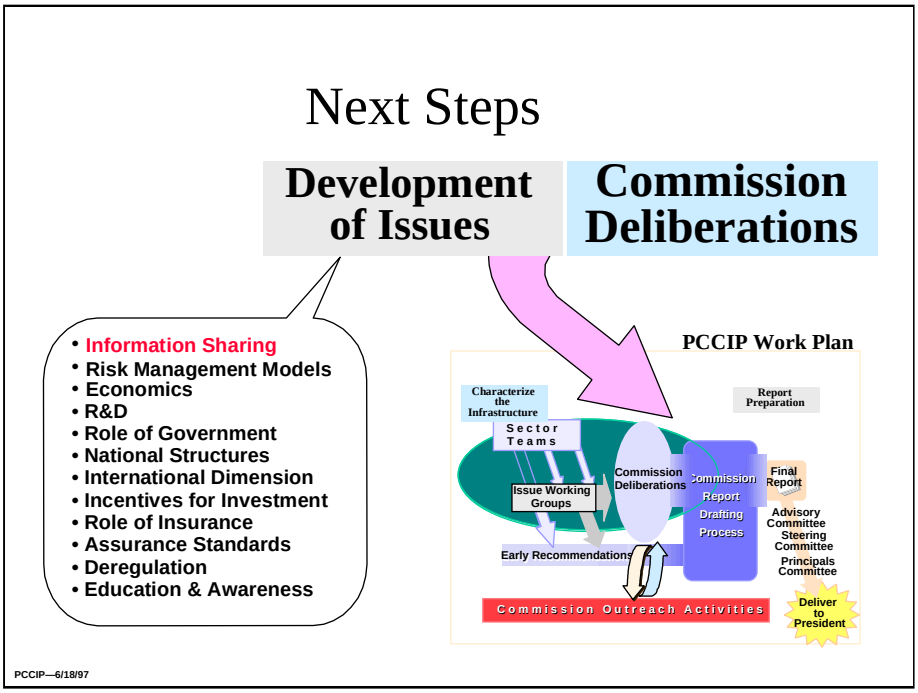


Consequences of Information "Stovepipes"

Although the Commission's work is still in progress, the need for better information flow within the Federal government, and between government and the private sector is readily apparent. The consequences of the current situation are summarized above.

There are no adequate interagency or public-private mechanisms for sharing and correlating data related to cyber attacks. Without shared information about intrusions, comparisons of aberrant events and other analyses cannot be performed. Neither the government nor the private sector has all the information needed to ascertain whether an attack is underway.

The Commission will seek to find a process for sharing such information among government agencies and the private sector.

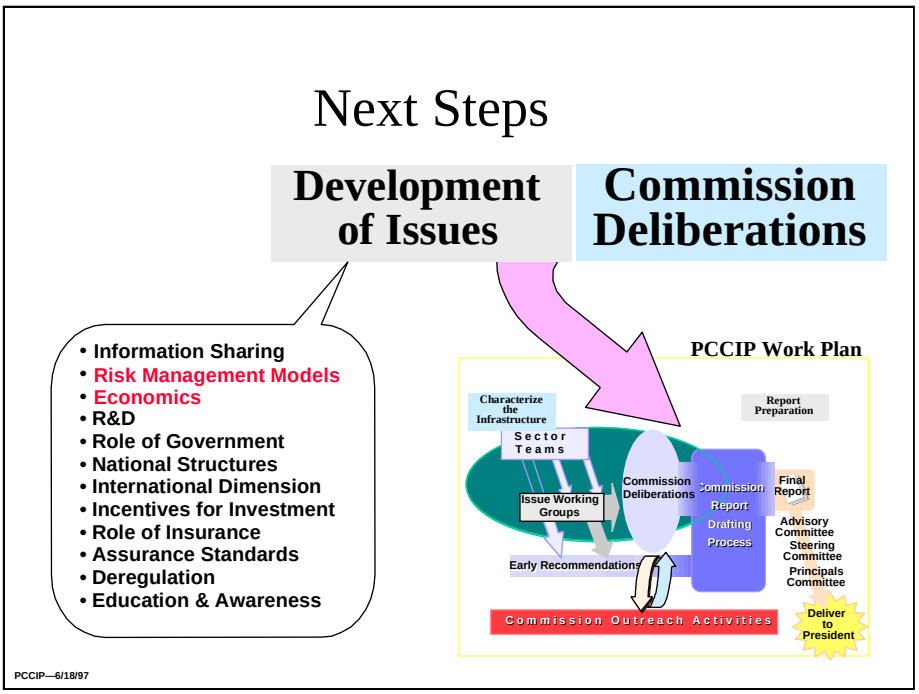


NEXT STEPS

We are currently engaged in the issue development phase of our work. Based on our characterizations of the infrastructures—which include identification of stakeholders, vulnerabilities and threats—initial explorations of interdependencies, and appreciation for the complexity of the infrastructures, we have identified issues that must be addressed to ensure the protection of the infrastructure in the future. Some of the issues we are examining are listed in the above schematic. Many cut across sectors. Issues are discussed in the paragraphs that follow.

Issue — Information Sharing in a Trusted Environment

The nature and consequences of information "stovepipes" have already been highlighted. There is an obvious and compelling need to create a trusted and mutually beneficial environment for information-sharing between the public and private sectors. What is less obvious is *how* to create a trusted environment. Government needs to provide infrastructure owners and operators as much information as it can about the nature of the threats they face, and the private sector needs to share information about attacks and other problems with the government so that government can better focus its efforts. We realize there is a great sensitivity to sharing information of this kind, but suggest there may be greater danger in not sharing it. Only when information is shared on a real-time basis is it possible to identify, warn, and respond to an attack, be it domestic, criminal, terrorist, or state-sponsored. In the months ahead we will be working to determine mechanisms that could protect government source-sensitive intelligence information and private sector information affecting reputation, consumer confidence, and liability.

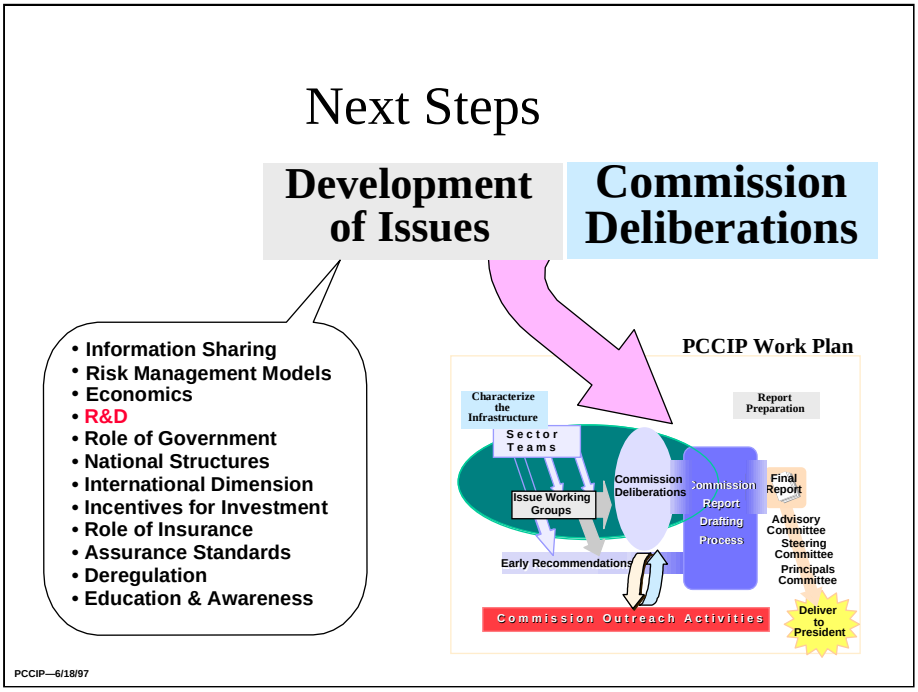


Issue — Risk Management

One of the salient characteristics of many critical infrastructures is their inter-dependency. This interdependence creates additional complexity. In earlier times, infrastructure reliability and assurance were generally the exclusive domain of the owner or operator in that particular industry. Now interdependency and complexity present new dimensions of risk, dimensions not fully reflected in the risk profiles used by infrastructures to guide investment decisions. We see the need to better accommodate emerging and future threats and vulnerabilities, in particular those that arise from our increasing interdependence and exposure to cyber interference.

Issue — Economics

Strengthening infrastructures will require increased investment, both public and private. Return-on-investment calculations usually drive critical infrastructure assurance expenditures. Fundamental concerns include economic costs of outages and failures, resources required for new technologies and new structures, and global competitive positioning of individual companies and the nation as a whole. The Commission is exploring an array of options for encouraging infrastructure assurance, including, but not limited to, investment incentives, regulatory changes, and the use of standards.

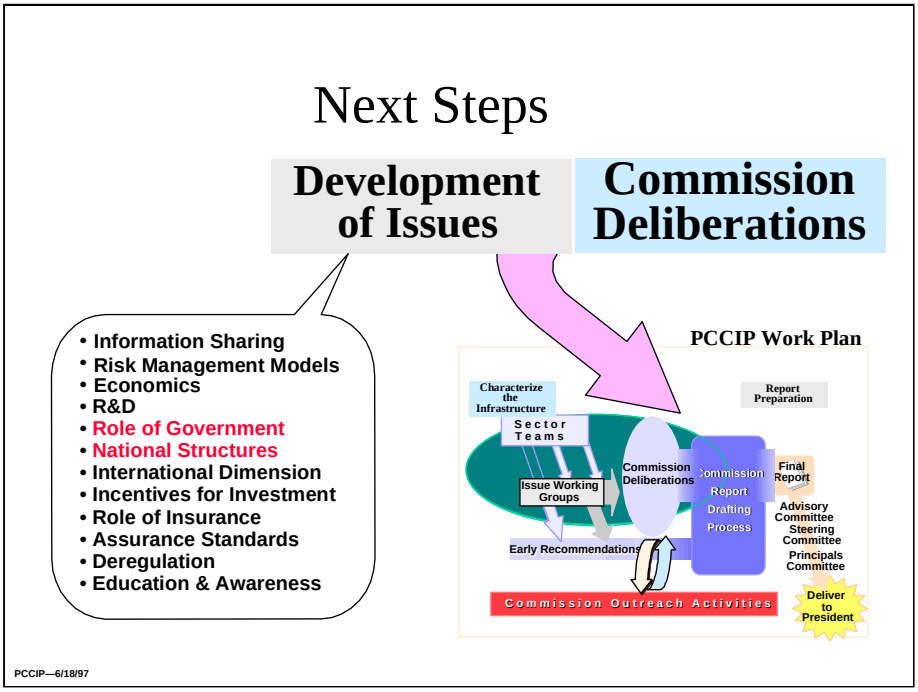


Issue — Research and Development (R&D)

One of the important lessons of our work is that technology is both a large part of the problem and an important part of the solution. America is a victim of its own success—our world leadership in technology, which makes possible instantaneous global transactions and just-in-time inventories, also creates vulnerabilities. As new systems are developed and implemented, hackers and other intruders quickly develop techniques to take advantage of or defeat them. Security features usually lag these new techniques, driven in part by the economic reality that the first new product to market is in the strongest position to gain the largest market share. The incorporation of robust security in new products delays their introduction. Hence research and development should be focused to provide better assurance tools for our increasingly interdependent systems and networks.

Government, in partnership with academia and the private sector, can promote the incorporation of assurance features into new system base architectures, as well as develop and provide security tools that can strengthen existing systems and architectures. Real-time intrusion detection tools are needed for preventing, responding to, and limiting damage from malicious intrusions. Current tools do not provide effective real-time monitoring, but instead support only “post-mortem” analysis of intrusions. More effective firewalls and widespread use of encryption can improve security in increasingly competitive marketplaces. Further, the research and development communities, government and industry, can focus technology to support market-driven standards for acceptable security performance.

Working with government agencies, we have an effort underway to identify existing infrastructure-related R&D throughout the government, industry and academia. The resulting database will be screened by committees of experts drawn from industry, universities, the National Laboratories, and government to assess the potential utility of the work underway and identify gaps in required technology development. We anticipate the outcome of this effort to be an agenda for research and technology development specially focused on protection of the critical infrastructures. An important aspect of this effort is to define the respective roles and responsibilities of the public and private sectors for the needed R&D.



Issue — Role of Government

The infrastructures are mostly owned and operated by the private sector. Market forces may go part way to assure delivery of vital services, but may not result in measures to cope with more severe attacks from terrorists or hostile states. The private sector must address protection against common-place intrusion, theft and fraud, but what about state-sponsored terrorism or hostile attack? What is the federal government's responsibility? Specifically, where is the line between private and public sector responsibility? The Commission will attempt to define these respective responsibilities.

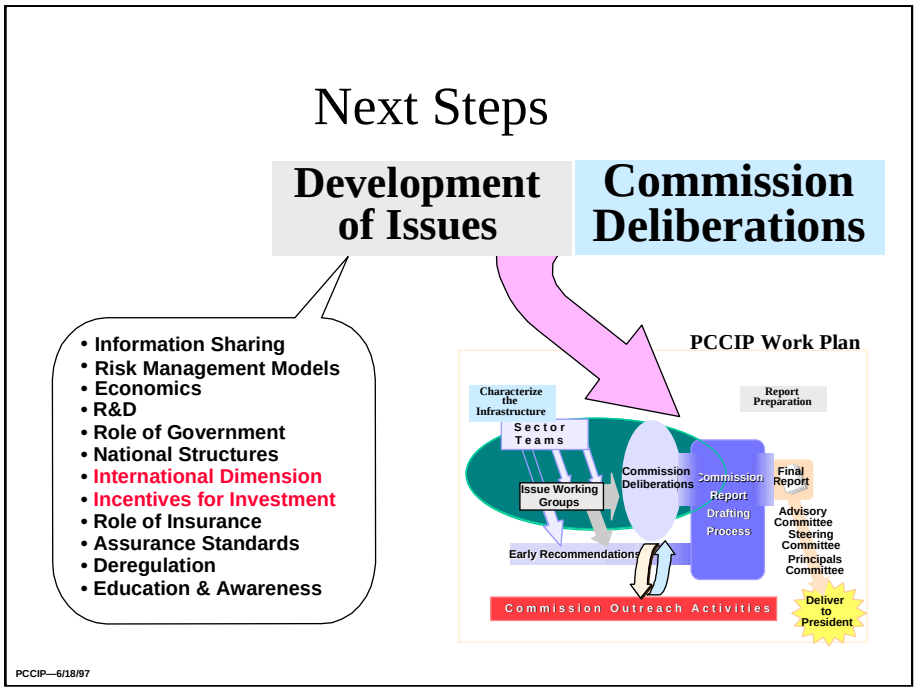
Issue — National Structures

Given that the federal government does have a role in infrastructure assurance, developing a national policy and implementation strategy requires an appreciation for what national structures are needed to assure the availability of the critical infrastructures today and in the future. We are therefore examining current structures and developing ideas for change. The information-sharing findings described above weigh heavily in this effort, since the structures recommended must accommodate public and private interests and must, as well, assure our strong democratic traditions and free market enterprise system into an uncertain future.

Current authorities and responsibilities for protecting the infrastructure provide the point of departure for effective analysis of structural needs. In addition to summarizing current authorities, we will survey current regulatory policies, methodologies, and practices throughout the nation.

"Who's in charge?" of responding to a cyber attack on the US is not a rhetorical question. Initial investigations reveal ambiguity in the alignment of responsibilities among law enforcement, intelligence, and national defense communities, particularly if an attack comes from or passes through another country. Ambiguities exist within and among levels of government and between government and the private sector. We have interviewed former senior officials, and we convened a focused panel of senior people to assist us in our thinking about how responsibilities might be assigned and shared.

The need to share information and provide tailored analysis has been described above. An issue team is developing options for sharing information among public and private sources, and for centralized analysis to provide operational warning of attacks on the infrastructures, particularly in the cyber arena. We will explore government-private sector models and recommend structures to accomplish this important mission.



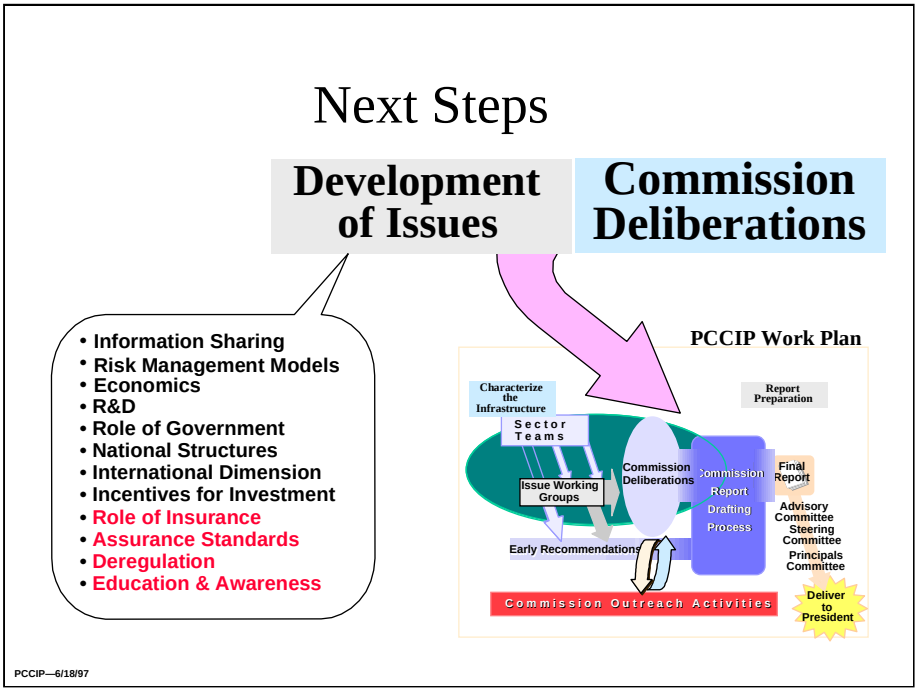
Issue — International Dimension

Technology and global markets extend the problem of infrastructure assurance well beyond our own borders. In the contemporary political and business climate of transnational market economies, global outsourcing of core functions, and multinational ownership of key infrastructure elements, secure operating standards and other rules are needed to promote the reliability of electronic information moving across borders. Global regulations and standards have been part of international trade, finance, communication, and transportation for over a century. Some of these regimes are private, and some are intergovernmental. Their form and method vary across sectors—air traffic control standards, for example, are strictly defined, while banking regulations are more loosely defined. Nevertheless, their common purpose has been to facilitate transnational commerce and communication. What sort of international agreements are needed for the global infrastructures? Are there models or examples of how domestic policies regarding infrastructure development convert to multinational standard-setting?

International action may also be needed on the national security side. A cyber attack can be launched from any place on the globe. What laws apply? A country hostile to the United States and wishing to disrupt or destroy our infrastructures could conceivably mount an attack from the territory of our friends and allies, or even from within the United States itself. What safeguards, then, are required to protect our critical infrastructures from unauthorized foreign intrusion? Are international agreements needed? If so, how should we proceed?

Issue — Incentives for Private Sector Investment

Given that private owners and operators have a key role in protecting the infrastructures we depend on, another important public policy issue is whether government should provide incentives for the private sector to invest in infrastructure protection. What will encourage companies to address vulnerabilities? How should incentives be structured?



Issue — The Role of Insurance

The Commission is exploring what role the insurance industry can and does play in achieving higher levels of infrastructure service delivery.

Issue — Assurance Standards

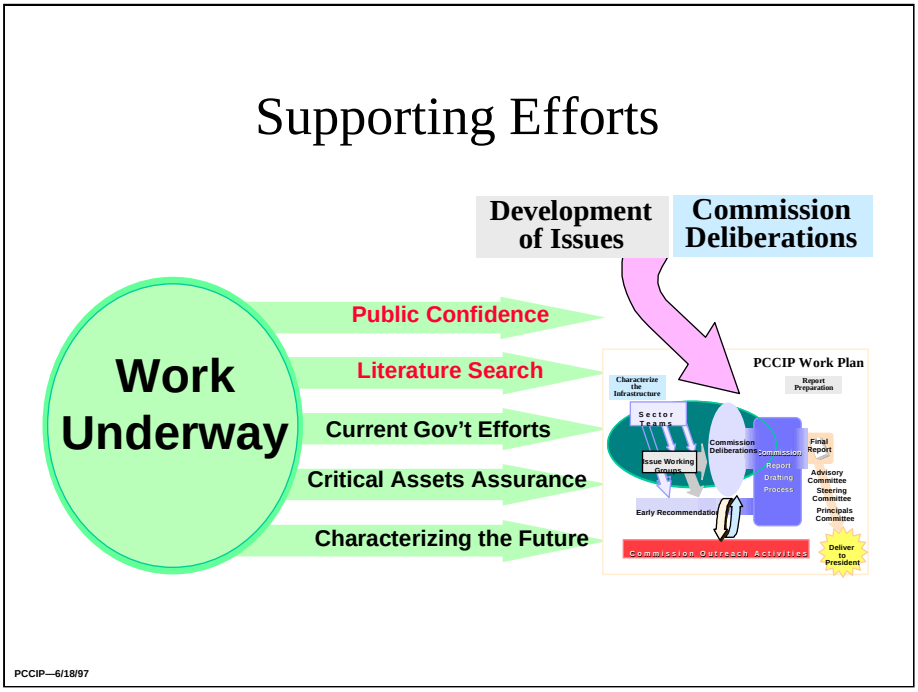
We are also exploring the role of standards in infrastructure assurance. Should there be standards of service delivery? If so, who should develop them? How should they be enforced?

Issue — Deregulation

Deregulation of the electric power industry may have implications extending to other critical infrastructures. For example, a company or factory that previously depended on a single electrical company for its power needs may soon be buying power that is generated by one company, transmitted across the country by another, and distributed locally by yet another. Each of the owners and operators involved in getting power to the customer has less control over the reliability of service than did the previous regulated operator who controlled the entire generation, transmission, and distribution system. In the future, when a peak load occurs, the control system will search for a source to accommodate the need. If such a source cannot be found, service may be interrupted, with obvious consequences for the customer. These new challenges must be addressed.

Issue — Education and Awareness

The telecommunications and computer processing systems and networks that tie infrastructures together have emerged in the last 15 to 20 years, with growth especially rapid in the last five. There is a large population of managers who lack formal schooling in information technologies and are learning by doing. There is also a younger population, brought up with computers, that is fluent in information technology but less experienced in other aspects of business. The accelerating growth of the information infrastructure demands that we adjust the educational system to close this gap.



SUPPORTING EFFORTS

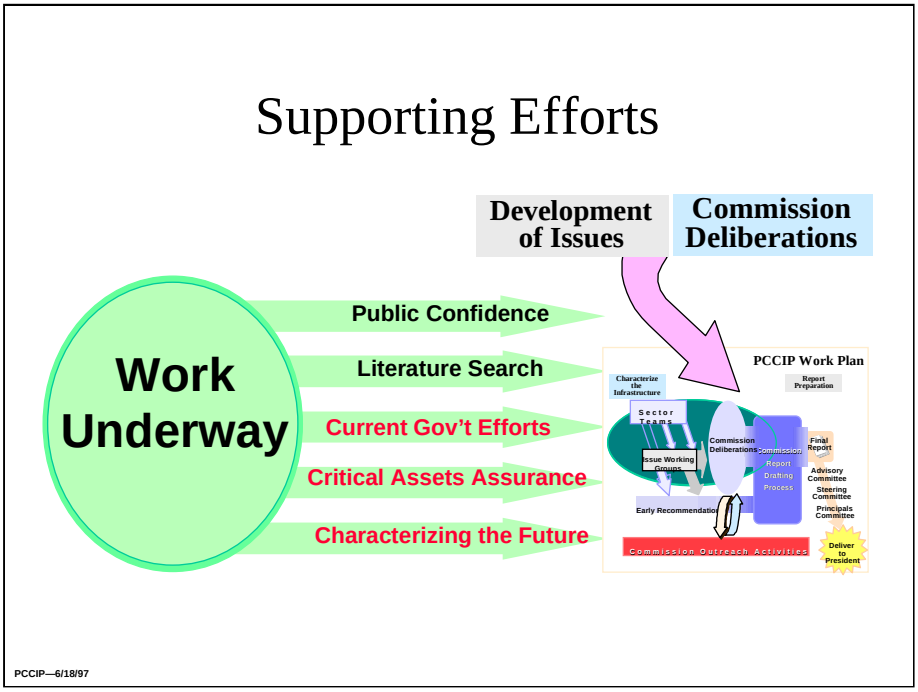
While the issues just described will likely lead to Commission recommendations, there is a great deal of additional supporting work underway. Some examples are described below.

Public Confidence

The loss of public confidence can turn relatively minor events into disasters of national proportion. The stock market collapse of 1929 led to a loss of confidence that contributed to the Great Depression of the 1930s. Public confidence is an asset that is essential to the health and vitality of our economic and social systems. Therefore, an important area for investigation involves public confidence and business trust, and their dependence on the critical infrastructures. Toward that end, we are surveying infrastructure stakeholders including the general public to assess the role of public confidence and its elasticity with regard to the infrastructures.

Literature Search

To ensure we have an understanding of the breadth and depth of work already done in related fields, and to appreciate the ideas already developed or proposed, an intense literature search was initiated early in the research phase. It continues in both unclassified and classified areas.



Current Government Efforts

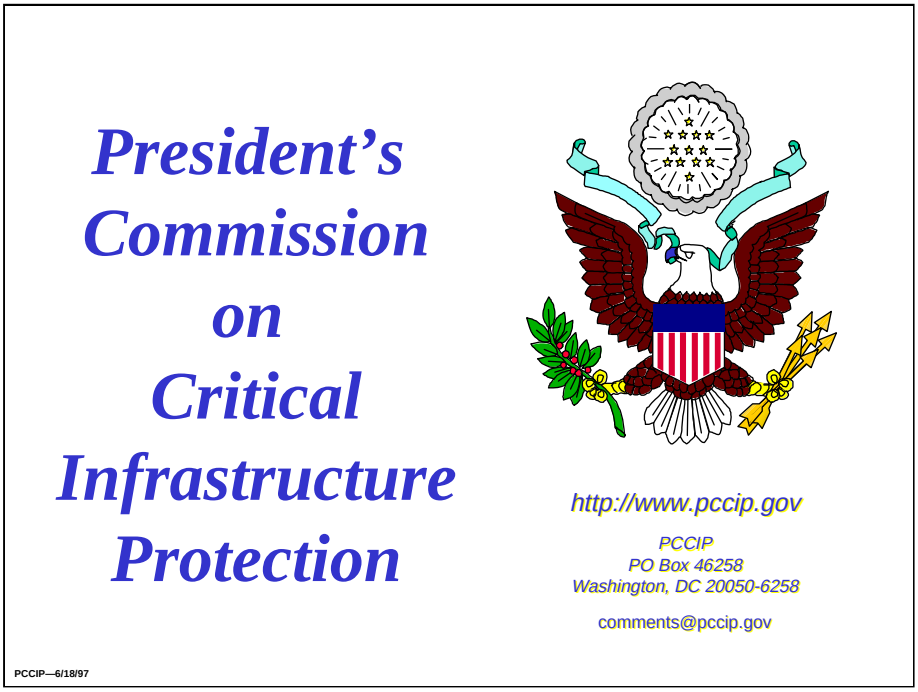
Government involvement in protection of critical infrastructures, particularly with regard to cyber threats, has been diffused throughout the federal government and other levels of government. To ensure that the Commission's recommendations reflect an accurate understanding of what is already underway, we are surveying all government agencies for related activity. The work of the Infrastructure Protection Task Force is expected to help us achieve this aim.

Critical Asset Assurance Programs

Critical asset assurance programs are underway in varying degrees throughout the government. The Department of Defense program appears to be the most robust. We are reviewing such programs and intend to consider the results in our recommendations.

Characterizing the Future

We will strive to ensure that our recommendations are adaptable to a future fraught with fast-paced change and quickly emerging threats to national interests around the globe. This is a particularly challenging assignment because of rapid advances in the information technologies our critical infrastructures rely upon.



CONCLUSION

This overview briefing summarizes the efforts of the President's Commission on Critical Infrastructure Protection. Consistent with our work plan, the Commission's efforts are becoming more tightly focused as we move toward deliberations and decisions about our recommendations to the President. At the same time, however, our need to maintain the dialogue with all infrastructure stakeholders continues. We are heartened by the strong and positive response to our many meetings with public and private representatives. All have indicated that there are threats, many new, to the infrastructures on which the economy and the security of the United States depend. All have noted the growing importance of international activities and the need for telecommunications and information infrastructures to facilitate these international efforts.

The respective private and government efforts to address infrastructure problems by specific infrastructures have served the country well in the past. However, the evolving threat, rapidly growing interdependence of infrastructures, and growing importance of international commercial activities emphasize the need for a reevaluation.

We are under no illusions that the Commission's recommendations can solve every aspect of every infrastructure problem. Instead, we see our strategy and recommendations as a point of departure for a continuing collaborative effort between government and the private sector.