

Securing Oil and Natural Gas Infrastructures in the New Economy

A Report of the
National Petroleum Council

This is a working document
as approved by the
National Petroleum Council
on June 6, 2001

This document is subject to final editing.

The final version of the Executive Summary
will be posted
when the full report is published in July.

Executive Summary

June 6, 2001

Executive Summary

INTRODUCTION

Based on the finding of a growing potential vulnerability, the President of the United States issued, in May 1998, a directive outlining the Administration's policy on critical infrastructure protection. An accompanying White Paper to the directive states:

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Study Request

In response to the President's policy directive, the Secretary of Energy requested the National Petroleum Council's (NPC's) advice "on cooperative approaches to protecting the critical infrastructure of the United States oil and gas industry."

In his April 7, 1999 letter, the Secretary specifically asked the Council to:

- Review the potential vulnerabilities of the oil and gas industries to attack, both physical and cyber
- Provide advice on policies and practices that industry and government, separately and in partnership, should adopt to protect or recover from such attacks.

Study Organization

The NPC established the Committee on Critical Infrastructure Protection to respond to the Secretary's request. The Committee was chaired by Richard B. Cheney, Chairman of the Board and Chief Executive Officer, Halliburton Company, until August 16, 2000. He was replaced by David J. Lesar, Chairman of the Board, President, and Chief Executive Officer, Halliburton Company. Eugene E. Habiger, then Director of the Office of Security and Emergency Operations, U.S. Department of Energy, served as the Committee's Government Cochair. A Coordinating Subcommittee was formed to assist the Committee in conducting the study and preparing a draft report for the NPC's consideration. This Subcommittee was chaired by Charles E. Dominy, Vice President, Government Affairs, Halliburton Company. Paula L. Scalingi, Director of the Office of Critical Infrastructure Protection, U.S. Department of Energy, served as the Subcommittee's Government Cochair.

Background

Over the past decade, the world has been changed by the information technology and telecommunications (cyber) revolution. As a result of these changes, global institutions have become more effective and productive.

Because of the pervasive use of cyber systems, they have become an interwoven part of the critical infrastructures. The United States, as does the rest of the world, faces an increasing number of threats to its infrastructures that are essential in times of peace and war. The threats faced are not only the traditional ones of natural disasters, human error, and attacks on physical assets, but now include threats to the cyber systems upon which today's economy is so dependent.

In the past, the oil and natural gas industries have effectively protected physical facilities. The protection of cyber systems has not kept pace with companies' ever-increasing dependence on them. The oil and natural gas industries have undertaken this study to better understand potential vulnerabilities and study methods for mitigating them.

Among the initiatives undertaken by the federal government related to infrastructure protection, two form the basis of the request for this study: the President's Commission on Critical Infrastructure Protection and Presidential Decision Directive 63. Undoubtedly, there will be more efforts in this area as the use of cyber-based systems expands globally.

The President's Commission

In July 1996, the President of the United States established the President's Commission on Critical Infrastructure Protection. The Commission's purpose was to assess the vulnerabilities of existing infrastructures and to recommend a comprehensive national policy and implementation strategy for protecting our nation's critical infrastructures. In its October 1997 report, *Critical Foundations: Protecting America's Infrastructures*, the Commission identified eight critical

infrastructures that are considered to be so vital that their incapacity or destruction would have a debilitating effect on our defense and economic security. These infrastructures are information and communications (telecommunications), banking and finance, water supply, electric power, oil and natural gas, transportation, government services, and emergency services (including medical, police, fire, and rescue).

Since many of these critical infrastructures are owned and operated by the private sector, as is the case for the oil and natural gas infrastructure, it is essential that the government and private sector work together. This theme of partnership in addressing critical infrastructure protection needs was embraced by the Commission and emphasized in its final report, *Critical Foundations*.

Presidential Decision Directive 63

In May 1998, President Clinton issued Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*, which built on the recommendations of the President's Commission that called for a national effort to ensure the security of the nation's critical infrastructures. The goal of the decision directive was that critical infrastructure protection programs would reach "initial" operating capability in the year 2000, and full capability no later than 2003.

The directive provided a framework for working with the identified critical infrastructure sectors to develop individual plans and meet the directive's goals. Each sector would be led by their governmental regulatory department or agency. The "lead agency" would appoint a "sector coordinator" to work with each of their sectors.

The energy sector's lead agency is the Department of Energy. The Department of Energy asked the North American Electric Reliability Council to be the electric power sector coordinator. As an interim measure, the National Petroleum Council was asked to be the sector coordinator for the oil and natural gas industries. At the

request of the Department of Transportation, oil and gas pipelines were added to the area being addressed by the National Petroleum Council. As outlined in this study, others in the oil and gas industries will assume the role of sector coordinator when this study is forwarded to the Secretary of Energy.

Status of Federal Critical Infrastructure Protection Activities

In February 2001, President Bush submitted to Congress a report on the status of federal critical infrastructure protection activities.¹ The report also reviewed government and industry progress toward the objectives outlined in Presidential Decision Directive 63.

Study Report

This NPC report suggests actions for identifying and reducing infrastructure vulnerabilities within the oil and natural gas industry sector. It raises the level of awareness and understanding of these new critical infrastructure protection challenges within our industry and government. It presents the business case for moving forward in this new business environment, adopting critical infrastructure protection thinking as part of the foundation of acting in the best interests of a company. It identifies the issues and the steps forward that the oil and natural gas industries and the government will need to implement, in partnership, to ensure the integrity and continuity of the industries' infrastructure.

This report's recommendations are intended to be dynamic, reflecting the fact that the industry is in the midst of significant change. Even the understanding of critical infrastructure protection is still evolving. While the Secretary's letter specifically mentioned attacks, the scope of the study has expanded beyond that to include many potential disruptions and vulnerabilities. Energy infrastructures are

¹ http://www.ciao.gov/CIAO_Document_Library/CIP_2001_CongRept.pdf.

inextricably linked with other critical infrastructures, and, as a result, a holistic perspective on critical infrastructure protection is essential.

The National Petroleum Council recognizes that some of the issues addressed in this report must be explored in greater depth and that some of the recommendations may warrant follow-on investigation. It is the intent of the NPC that this report will provide a basis for constructive debate and serve as a foundation for the next steps in developing a viable blueprint for the energy industry and the nation.

FINDINGS

New Business Environment and Critical Supporting Infrastructures

Society has moved from a model of gradual change to one of exponential change because of development and reliance on cyber and other electronic systems. Such change is pervasive, throughout every aspect of business, government, and personal lives. Advances are expected to continue at an exponential rate, affording no return to the traditional model. Significant advances in information technology (IT) and telecommunications are enabling the change to a new, interconnected, global economy. With these advances, the nature of security issues is expanding to include threats and vulnerabilities associated with cyber and other electronic systems. The new economy is supported by and increasingly dependent on several critical infrastructures as identified by the President's Commission on Critical Infrastructure Protection:

- Oil and natural gas
- Electric power
- Information and communications (telecommunications)
- Transportation
- Banking and finance

- Water supply
- Government services
- Emergency services (including medical, police, fire, and rescue).

Oil and Natural Gas Industries in the New Economy

The oil and natural gas industries provide almost 62% of the energy used in the United States. These energy sources are vital and directly underpin much of the U.S. economy. The oil and natural gas industries are experiencing the same exponential changes as the rest of the economy. While this sector's physical footprint appears the same—wells, gathering systems, processing facilities, transmission systems, and distribution systems—the approach to operating the industries, both from a physical and business perspective, has changed. Many of the changes are directly linked to the burgeoning use of electronic communications and have resulted in modifications such as the use of advanced electronic control systems and business arrangements based on electronic transactions. For example, systems that control operating processes within refineries, along pipelines, and in producing fields were previously closed and proprietary. These control processes are now moving toward open architecture and commercially available software. Also, much of the raw material and product that is purchased and sold is accomplished using electronic-based futures markets. Because of the alterations in equipment configuration and corporate re-engineering, many of the changes are essentially irreversible.

Today, organizational changes such as mergers, alliances, and joint ventures have resulted in organizations that no longer resemble the energy companies of the past. These changes have resulted in the transformation of service companies, and blurred the lines between traditional oil, natural gas, power, and pipeline companies.

New Electronic and Interconnected Economy

Information is becoming universally and instantaneously available. This is leading to a strong global business network available to all regardless of size, financial strength, or purpose. The growth in the availability and dependence on electronic systems, due to the expectation of synergy, has created a marked increase in the interdependence of entities. Information is more transparent, difficult to protect, and easily transferred. These electronic systems are interconnected globally, making traditional physical boundaries less important.

The critical infrastructures outlined by Presidential Decision Directive 63, including those of the oil and natural gas industries, have a common dependency on IT and telecommunication systems. Additionally, electric power and water supply systems use supervisory control and data acquisition (SCADA) operating systems similar to those used by the oil and natural gas industries. As time passes, an increasing amount of information is available in an electronic format. Consequently, information is subject to either accidental or deliberate corruption, theft, or denial of access. Organizations have to deal with the challenge of information assurance as a condition of doing business in today's world.

Vulnerabilities, Consequences, and Threats

The introduction of cyber technologies has increased risks in the oil and natural gas industries. The traditional security approach has been to physically protect personnel and property from human error or natural disasters. Emergency plans to deal with such events remain in place. However, processes are inadequate to deal with the changes that are accompanying the increased dependence on cyber and other electronic systems. This critical reliance is a recent phenomenon resulting in new threats and a high level of vulnerability because the development and adoption of processes to ensure security in this area has not kept pace. The new weapon is electronic bits, versus bombs in the old paradigm.

In this new paradigm, individuals and groups, from hackers to organized terrorists, have the ability to simultaneously attack multiple sites. Because the success of such attacks are often disseminated to a wide audience, they often become the blueprint for additional attacks. Beyond cyber attacks, human error and normal system failures continue, which because of the growing level of interconnectivity of systems, have the capability of doing far more damage than in the past. The consequences of these attacks and failures are more difficult to predict, and potentially more extensive.

The reliance on cyber technologies creates the opportunity for interrupted communications, false or misleading transactions, fraud, or breach of contracts, and can result in potential loss of service, loss of stakeholder confidence, or the failure of the business itself. The due diligence standards in this new environment remain ill defined and transitory. Also, when infrastructure disruptions occur, conflicts of interest can develop between the various entities involved, that inhibit response, restoration of service, and future infrastructure protection.

Risk Management and Vulnerability Mitigation

In addressing risk management and vulnerability mitigation, the study concluded that companies in the oil and natural gas industries will benefit from conducting periodic vulnerability assessments of their own systems and operations, both physical and electronic. In many situations, the global nature of doing business today has resulted in an intertwining of cyber systems between organizations. Therefore, assessments of partners' vulnerabilities, with joint vulnerability mitigation efforts, may be important to protect business relationships. The vulnerability of interdependencies with other infrastructures should also be an inherent part of these assessments.

Response and Recovery

Most companies understand and are able to handle their own physical infrastructure disruptions. Cyber response and recovery capabilities and processes are not as mature as those developed to handle physical incidents. Increased use of automation, increased interconnectedness, just-in-time business models, and interdependencies can potentially result in regional, national, or international incidents and impacts. The increasing use of information and communications technology and the potential for these broader consequences are generating new challenges for response and recovery planning.

These increasingly complex response and recovery environments dictate that plans be periodically tested to ensure they will manage emergencies and reduce risk for all stakeholders. This new business environment dictates that companies include key stakeholders, such as business partners, suppliers, customers, and representatives from local and state governments in response and recovery tests and exercises.

When infrastructure disruptions occur, the roles and responsibilities of local, state, and federal governments often conflict. These conflicts of interest regarding jurisdiction impede timely restoration of service and can also inhibit timely development of infrastructure protection processes. Timely and actionable information is important for effective response to threats or incidents, as well as for successful recovery actions. Companies can benefit by having an effective internal information sharing mechanism to receive, analyze, and disseminate incident information to enhance response and recovery.

Information Sharing and Sector Coordination

In the oil and natural gas industries, only limited capabilities exist for sharing information on physical and cyber incidents, threat assessments, and vulnerabilities. Receipt of real-time information is critical in protecting the oil and natural gas

infrastructures, and rapid reporting of incidents is vital. A broader base of participation in information sharing enhances the timely flow of information. Sharing of information, however, raises uncertainty concerning liability, privacy, and antitrust issues. Centralized collection of specific vulnerability data could create a source of information that could be used for nefarious purposes. Under current law, there is uncertainty about the government's ability to keep information from public release. Such a release could result in loss of investor confidence, shareholder value, and business reputation.

This study concludes that information sharing related to threats and responses to threats would be beneficial to the oil and natural gas sector. Of the three general models for implementing an information sharing mechanism (reliance on industry staff, use of an industry-directed service provider, or a hybrid government/industry management), the industry-directed service provider model is the most efficient and appropriate for the oil and natural gas sector.

A permanent sector coordinator should be designated to lead the critical infrastructure information sharing effort and to be the focal contact point for other oil and natural gas industries critical infrastructure issues.

Legal and Regulatory Uncertainties in the New Economy

There are many legal uncertainties regarding the electronic aspects of the new economy. While laws and legal procedures are emerging, they have yet to be tested by the judicial process in any significant way. International law, where it exists, often varies from U.S. law and is either more or less stringent, or conflicting. Risks associated with cyber and other electronic systems often involve intangible, highly uncertain potential losses.

Corporate structures are changing, with mergers, joint ventures, alliances, and increased dependence on outsourcing. Consequently, the oil and natural gas industries have become more reliant on contract law. A variety of efficiency moves

are now commonplace and often involve non-U.S. entities making national differences in legal approach an added complexity. There has been a shift of the energy enterprise among providers, marketers, and systems. These accelerated changes in ownership along with changes in industry roles and responsibilities are occurring throughout the industry. Business restructuring is moving from the traditional “wires” and “pipes” business to non-traditional investments (e-business activities). All of these changes impact the robustness of the oil and natural gas infrastructure.

Research and Development

When considering critical infrastructure protection research and development (R&D) in areas such as information technology, the oil and natural gas industries do not have unique expertise, and primarily rely on commercial providers to conduct the necessary R&D. The government conducts a broad range of R&D activities in this area, the results of which could be used to meet infrastructure protection, mitigation, and response and recovery needs by the oil and natural gas industries. This includes R&D on information assurance and other national security areas. The government should assure through consultation with industry that R&D pursued reflects industry and government needs, and is not redundant with private-sector efforts. There needs to be an effective method for providing greater technology transfer to industry, particularly from its national defense and other classified research programs.

The Successful Y2K Model

The Y2K experience provides a good “go forward” model for government and industry. It emphasized the risks faced by the government and private sectors due to the interconnectivity and interdependency of their respective critical infrastructures. Y2K also demonstrated that significant challenges to national interests could be addressed through information exchange, the removal of legal barriers, and elimination of the fear of federal, state, and local government intervention.

RECOMMENDATIONS

Based on the findings of this study, the National Petroleum Council recommends that industry and government take the following specific actions to better protect the critical infrastructures of the oil and natural gas industries. The business case for taking proactive measures is persuasive and instructive. The energy industry cannot do this alone. The challenges of the new economy and the increasing interdependencies among and within our infrastructures necessitate that industry must work with other sectors, and with federal, state, and local governments.

Vulnerability Assessments, Information Assurance Process, and Planning Recommendations

- **Vulnerability/Risk Management Assessments.** Each company should regularly conduct vulnerability assessments of its own systems and operations and take action as appropriate. In addition, each company should conduct assessments of its partners' vulnerabilities. Risk management processes should be reviewed to ensure that both electronic and physical security is included.
- **Information Assurance Process.** Industry and government should advocate the development, adoption, and implementation of global IT management processes to reduce vulnerabilities of the cyber and other electronic systems on which the oil and natural gas industries are dependent. A good example of such a process is the International Standards Organization (ISO) 17799, "The Standard for Information Security Management."
- **Response and Recovery Planning.** The oil and natural gas industries should enhance their response and recovery plans as they relate to information technology system disruptions, while continuing their traditional role of maintaining and implementing plans for disruptions to physical facilities. Individual companies should consider engaging in regional response and recovery planning and exercises to deal with disruptions to physical and cyber infrastructures resulting from natural disaster, system failure, human error,

or sabotage. Additionally, industry must take into account the challenges of the new business environment, including infrastructure interdependencies, and enhance response plans to ensure they are adequate and coordinated with other infrastructures, regional, state and local emergency response programs.

Information Sharing and Sector Coordination Recommendations

- **Information-Sharing Mechanism.** The oil and natural gas industries should establish a secure information-sharing mechanism to collect, assess, and share with its members information on physical and electronic threats, certain vulnerabilities, incidents, and solutions/best practices. This mechanism also would gather and receive information from government, technology providers, and other information sharing mechanisms. The specific type of mechanism recommended is commonly called an information sharing and analysis center (ISAC). Of the three general models for ISACs, the industry-directed service provider model is the most efficient and appropriate for the oil and natural gas sector. Under this model, the oil and natural gas industries' ISAC would likely be a non-profit, cooperative organization.
- **ISAC Membership.** Under the current law and legal environment, the ISAC would only share information within the oil and natural gas industries. Therefore, membership would be initially restricted to private-sector companies operating in the oil and natural gas industries. Consideration should be given to allowing industry associations to join in order to disseminate information to smaller oil and natural gas companies. Private companies who share similar technologies, such as the electric and water supply industries, may be encouraged to join at a later time. Eventually this may be extended to other entities, as interrelationships become apparent.
- **Implementation.** The oil and natural gas industries will take the lead in establishing a board, which will investigate, develop, and implement an ISAC for the sector.

- **Sector Coordination.** While no organization represents all segments of the oil and natural gas industries, it is recommended that the Secretary of Energy formally acknowledge the designee of the governing body of the oil and natural gas industries ISAC as the sector coordinator.

Government Action Recommendations

- **Legislative Actions.** The federal government should enact legislation to facilitate information sharing with and among sector components. Communications with government involving critical infrastructure protection information should be exempted from the provisions of the Freedom of Information Act. Also, legislation should be enacted to provide liability and antitrust relief for critical infrastructure protection information sharing similar to the law covering Y2K activities. While the need for individual privacy is recognized, the need must be balanced against the critical nature of protecting infrastructures as regulations are formulated and laws are enacted.
- **Access to Law Enforcement and Intelligence Information.** The industry would benefit from real-time, relevant vulnerability and threat information that is only available to government under current conditions. Government and industry should work together to develop processes that ensure the sharing of relevant information.
- **International Initiatives.** The federal government should use all means available to encourage countries to enact globally consistent laws addressing the interconnected, electronic commercial marketplace. The government could use the same approach to encourage the development and adoption of global technical standards and uniform business practices to reduce the vulnerabilities of cyber and other electronic systems. The government should undertake collaborative efforts with other nations to enhance global infrastructure assurance.

- **Holistic Approach to Energy Critical Infrastructure.** All components of U.S. energy sectors should be viewed as a single energy infrastructure in the implementation of critical infrastructure protection. U.S. energy components (i.e., oil, natural gas, electric power, other energy sources, and their transportation modes) are converging with each other in the marketplace.
- **Response and Recovery Activities.** Federal, state, and local governments should ensure coordination of response and recovery activities for significant disruptions that require actions beyond the capabilities or purview of individual companies in the oil and natural gas sector. Preplanning should be undertaken to minimize jurisdictional conflicts among government entities during the response to and recovery from a major emergency.
- **Research and Development Activities.** Government-funded research and development should address national security and other key critical infrastructure protection, mitigation, response, and recovery needs that transcend individual companies in the oil and natural gas sector, with other areas being the focus of R&D by commercial technology providers. The federal government should work with industry to focus and prioritize its funding of critical infrastructure protection research and development. Government should also provide for the rapid transfer to the private sector of government-funded R&D applicable to critical infrastructure protection, especially in the information technology and telecommunications areas.
- **Continued Support for Critical Infrastructure Protection Initiatives.** The government should continue its critical infrastructure protection initiatives, working closely with the oil and natural gas industries and other critical infrastructures to protect the country's national security, economic health, and social well being. The government should be organized to effectively interact with industry on a broad range of mutual critical infrastructure protection issues.