MARCH 2003 / VOLUME 1, NUMBER 9

THE CIP REPORT

OIL AND NATURAL GAS ISSUE

CIP PROJECT STAFF

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Legal Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Meredith Gilchrest, *CIP Law and Policy Research Archivist / Outreach Program Manager*

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

George Baker, *Interim Director JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

Focus on Oil and Natural Gas

This issue of *The CIP Report* focuses on the oil and natural gas industry of the energy sector. The driving force behind the field of critical infrastructure protection-that a growing dependence on automated systems creates simultaneous efficiencies and vulnerabilities-is as true for oil and natural gas as it is for most other economic sectors.

The physical infrastructure of this sector has remained largely the same-wells, gathering systems, processing facilities, transmission systems, and distribution systems-but the way the sector does business has changed immensely due to the use of electronic control systems. Operating processes from the producing fields to refineries and pipelines to the sale of raw materials are dependent on electronic systems.

The industry has decades of experience in physical security, but the relatively recent threats and vulnerabilities introduced by cyber systems are difficult to harness. Since being identified as a critical infrastructure by the President's Commission for Critical Infrastructure Protection, the industry has been busy addressing the various components of assessment and vulnerability mitigation as well as consequence management.

In response to a request by the Secretary of Energy, the National Petroleum Council released a 2001 study entitled *Securing Oil and Natural Gas Infrastructures in the New Economy*, in which it recommended industry wide vulnerability and risk assessments, response and recovery planning, and an information sharing mechanism, as well as several recommendations for government action. Since release of the report, the industry has made significant strides in each of these areas. The American Petroleum Institute, along with industry partners and the Departments of Energy, Transportation, and Homeland Security, federal and local law enforcement, and the intelligence community, has built a strong public / private partnership. Some of the industry's activities include development of industry-wide security guidelines, the formation of the Energy ISAC, energy site and cyber inspections, and regional security workshops.

This issue introduces you to some of these initiatives, as well as other activities and issues the sector is facing.

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

Making Security a Priority in the Energy Industry

By Kendra Martin, CIO and Security Team Leader

American Petroleum Institute

"French Oil Tanker Hit By Terrorists," "Oil Workers Shot At In Yemen," "Saudis Thwart Planned Attack on Oil Terminal," "Energy Industry Gets Terror Alert."

The headlines are bringing home one of the harsh realities of the post September 11 era. Pipelines, refineries, tankers, offshore drilling platforms and the computers that drive them are in the sights of terrorist groups looking for ways to disrupt the American economy.

No one is more aware of the industry's vulnerabilities than the American Petroleum Institute and its member companies. And because of that, security specialists have spent long hours since September 11, 2001 helping companies protect themselves from the possibility of attack.

Even as New York and Washington were still reeling from the initial attacks, it became apparent that our industry needed to work closely with the many federal, state and local agencies responsible for the health, safety and security of people who live or work close to or on oil and gas facilities.

In dozens of meetings with federal officials over the past 16 months, API staff members and company officials discussed ways to improve the security of oil and gas facilities and to keep companies informed when there are reports of potential attacks.

In addition, companies reached out to local police and Emergency Service organizations to plan coordinated defenses, evacuation and medical treatment if terrorists target their facilities. This is especially true in cities like Houston where there are heavy concentrations of oil and gas facilities.

Kendra Martin

Meanwhile, security specialists from member companies and API staff met frequently with federal officials and the result was the publication in April 2002 of "Security Guidance for the Petroleum Industry," a 128-page road map for managers to use in assessing the vulnerability to attack of pipelines, terminals, refineries and drilling platforms. A new edition with updated guidance will be published mid-2003. These guidelines provide a framework for petroleum companies to develop site-specific security programs based upon their own unique needs and circumstances. The guidance contains the National Threat Alert Advisory System, including both general and specific protective measures that should be considered when there is a change in threat level.

Officials of the U.S. Department of Energy, the Environmental Protection Agency, the Office of Pipeline Safety and the Coast Guard were asked for suggestions in improving the original guidance. The document was publicly praised in a letter from Energy Secretary Spencer Abraham to Secretary Tom Ridge.

Over the last several months, the guidance document was distributed to hundreds of industry managers who have used it to make critical security improvements. They include sophisticated methods of verifying the histories of potential employees and tightening access to susceptible facilities. Companies have also instituted new ways of keeping track of fuel trucks enroute to industries and retail gas stations.

Industry executives also recognize that a cyber attack can be as devastating as a truckload of explosives. Our industry is heavily reliant on sophisticated technologies not only to locate and extract oil and natural gas, but for efficient operation of tankers,

(Continued, Page 11)

LEGAL INSIGHTS

by Emily Frye

Protecting Oil and Gas Infrastructures: A Classic Competitive Conflict Comes Face-to-Face with the Era of Terrorism

At a recent conference, a colleague from the electric-power ISAC shared with me his concern that an overweening focus on electricity within his sector overlooked today's foremost threat to the energy infrastructure: the oil and gas pipelines that connect raw resources into and through the United States.

His observation summarized quite neatly a problem that faces all critical sectors, but none more so than energy: protecting the assets that I own and control does not ensure my ability to function. Natural gas, of course, is used to generate electricity, so a pipeline disaster could disrupt electricity delivery in a multistate region - which, in turn, would disrupt all the appliances that operate using electricity.

The National Academy of Sciences estimates that the United States houses almost 880,000 oil wells, 161 oil refineries, 726 gas-processing plants, nearly 1.3 million miles of natural gas pipeline, and 220,000 miles of oil pipe - all extremely combustible infrastructure assets. Together, oil and natural gas provide over 60 percent of the U.S. energy supply. These assets are, unfortunately, attractive terrorist targets.

Combined with the obvious physical threat, which seems greater than ever following the permeability proven by September 11, is a sudden awareness of the compounded vulnerability posed by vulnerable Information Technology systems. Perhaps it is this vulnerability that has spurred the oil and gas industries, somewhat late to the game, to form an ISAC. Notably, the oil and gas ISAC has stated that it will focus initially on IT and telecommunications.

> ***...protecting the assets that I own and control does not ensure my ability to function...***

In June 2001, the report of the National Petroleum Council, Securing Oil and Natural Gas Infrastructures in the New Economy, urged each company in the sector to "regularly conduct vulnerability assessments of its own systems and operations and take action as appropriate." The report also directed that "each company should conduct assessments of its partners' vulnerabilities" [emphasis added]. Echoing this sentiment in the post-9-11 world, Thelen Reid and Priest observed in its February 14, 2003, issue of Energy and Infrastructure News that the "key challenges to the electricity and oil & gas industries" include "assessment of new potential liabilities" and "identification of and compliance with any new or pending legislation or proposed rules that require increased security procedures."

The difficulty in carrying out such recommendations, however, is very real. Nearly all players in the sector have seen their profits and value drop since 2000. The financial burden of carrying out risk assessments and subsequently implementing necessary protective measures is too great for any single company to bear - even in a time of plenty. Furthermore, the oil and gas sector is not a centralized industry. It is a sector characterized by a wide distribution of asset-ownership. Many thousands of owners and operators, with differing asset portfolios, operate independently of one another. Physical and system diversity have one advantage: an attack on one is not an attack on all, and an isolated incident at a single facility probably will not disable large numbers of users for prolonged periods.

Nonetheless, the National Petroleum Council's report

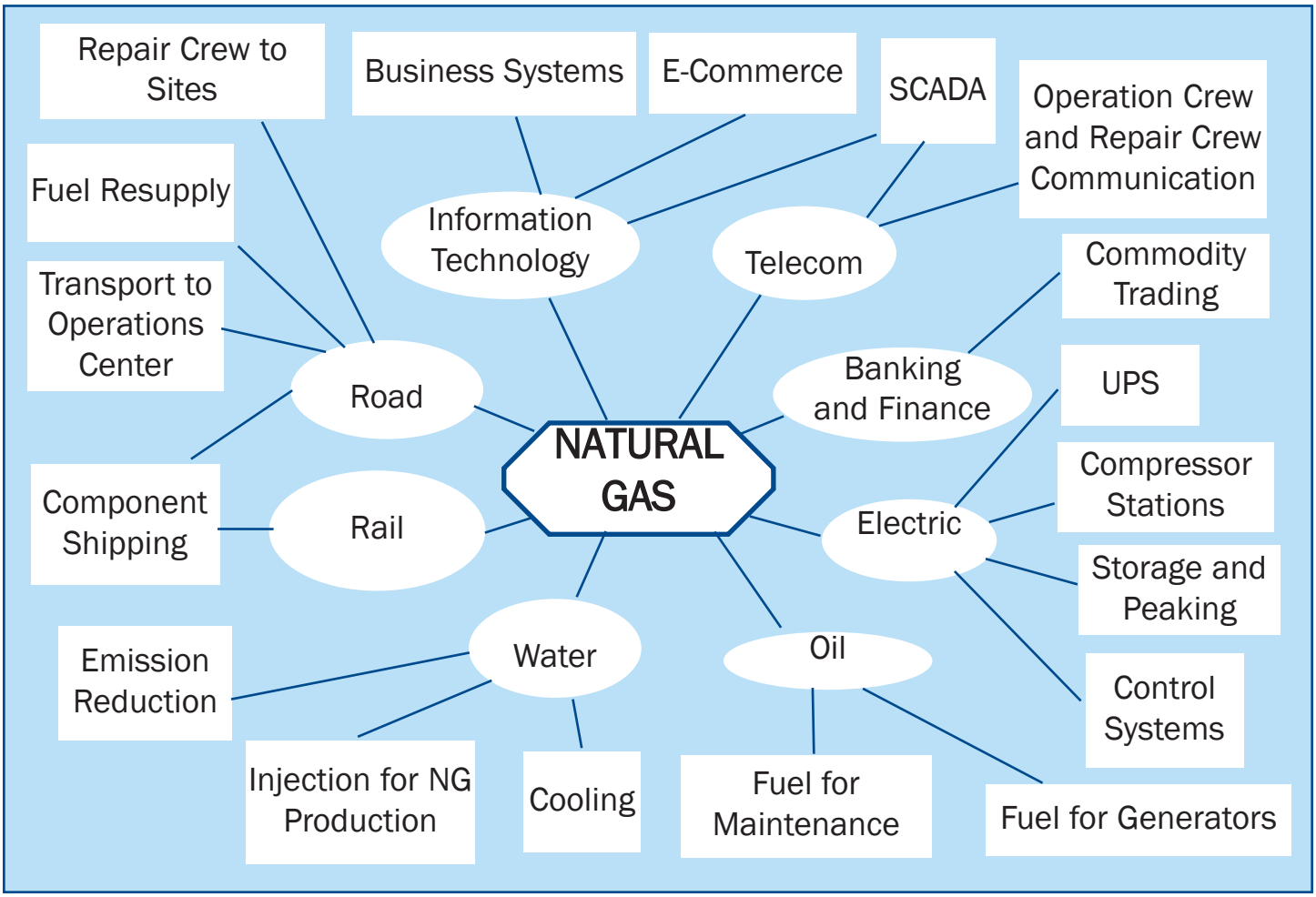
(Continued, Page 4)

(Continued from Page 3)
recognized that "all components of U.S. energy sectors should be viewed as a single energy infrastructure in the implementation of critical infrastructure protection." Yet in 2003, electric power and oil/natural gas each have their own ISAC, without an information-sharing or partnering agreement between them.

As the NPC's interdependency analysis shows, the sector's strength is also the basis of its information-sharing weakness: not only does the diagram below describe the challenge of protecting the sector as a whole - the subtext here is that it describes the challenge of protecting any given company's assets. Once completed, every company's interdependency analysis looks different. Its partners and customers are different, each participant holds a different ratio of criticality to the core provider, its information-technology systems are unique, and its total reliance on any given aspect of the system varies. What incentive does any given player have to cooperate, or share information, with any other?

Aside from civic responsibility or national pride, then - not to be underestimated in a time of war, and yet more often dispensable when the economy is weak - can an argument be made for joining forces? There is one: aggregate purchasing power for security solutions. The Federal Energy Regulatory Commission will be working with the Department of Homeland Security to monitor the relationship of energy and national security. As new regulatory developments lead to heightened security requirements, owner-operators can benefit from combining forces in the marketplace for security solutions. As long as nobody knows the next target, everyone pays. Just maybe, if we use some Wal-Mart wisdom, we can pay less.

❖



Helping to Reduce the Threat

The Energy Information Sharing and Analysis Center (Energy ISAC) is a secure, Internet based program by which energy sector companies and utilities can obtain and share important information about vulnerabilities, threats, intrusions, and solutions related to physical and cyber security. Energy ISAC is an aggregated single source for threat vulnerability and incident information and is an excellent tool to reduce an individual company's risk - and the industry's - through timely information exchange.

While we are still working to build and enhance the Energy ISAC, even in its early deployment, the industry has already seen benefits: quicker sharing of information, more robust cyber solutions, and closer collaboration with each other and our government counterparts.

Kendra Martin, American Petroleum Institute

Energy ISAC is a non-profit group that educates and helps protect members of the energy industry from threats to their facilities and operations. Through a grant from the U.S. Department of Energy (DOE), Energy ISAC provides the following services to at NO COST:

- 24 x 7 information monitoring and dissemination with alerts and warning pages, e-mails, and faxes from the Energy ISAC operations center.
- Physical vulnerability alerts and advisories from the FBI's National Infrastructure Protection Center, DOT's Office of Pipeline Safety, U.S. Coast Guard, Office of Homeland Security, and other government entities.
- Cyber vulnerability alerts involving enterprise software, major viruses, worms, and exploits from anti-virus vendors, research groups, internet security firms, associations and advisory groups.
- Information sharing and analysis among Energy ISAC participants via the Energy ISAC website (with an option to remain anonymous).
- Access to monthly intelligence audio conferences (nominal cost per call).

With the real possibility of future terrorist incidents, the information needed to determine individual company vulnerability risks and appropriate measures to take to protect our critical facilities has never been more important.

Through a partnership with the Department of Energy, the American Petroleum Institute, the American Gas Association, the Association of Oil Pipelines, the Interstate Natural Gas Association of America, the Independent Petroleum Association of America, the National Petrochemical and Refiners Association, the American Public Gas Association, and others in the industry, Energy ISAC offers an attractive, no-cost solution to strengthen any corporate security program.

More information can be found at the Energy ISAC website at www.energyisac.com. ❖

THE INFORMATION SECURITY WORK FORCE: The New Millennium

by
Allan Berg, James Madison University

(The first installment of a three part series)

The nature of the information security (IS) and Information Technology (IT) work force challenge has been the subject of much debate over the past several years. There are many conflicting views of the challenge, and even among those who agree on the nature of the challenge, there are conflicting views of what the best solutions are. The perception of the challenge tends to be shaded by the perspective of the observer.

For the most part, industry sees the problem as a worker shortage. Companies believe that there simply aren't enough people in the IT and IS occupations to meet the growing demand. Employee groups and advocates for employees, on the other hand, believe there are enough trained technical professionals, but industry has not tapped these existing labor pools. Economists argue that the IS work force challenge is the expected result of the rising importance of IS in our economy and the consequent demand for highly-skilled core IT and IS workers, and that, in the long run, market forces will fix the problem. There is merit to all three perspectives.

Two factors are chiefly responsible for creating the IS worker challenge. First, there has been sustained rapid growth in the demand for highly skilled IS workers-demand that has accelerated in recent years. This demand is the product of the Information Age and virtually every industrialized nations' economy has embraced IS for the security it brings to existing business functions, as well as for the new capabilities, products and services IT enables. As a result, demand for highly skilled IS and IT workers lead virtually all other occupations in demand for skilled workers and are expected to continue in the years ahead. Second, the variety and complexity of software and hardware products and their applications, together with the unique IS business requirements of each industry, have created intense demand for workers with unique combinations of information technology coupled with IS skills, experience and industry knowledge-expressed often by employers as needing "the right person, with the right skill, at the right time." The combination of time-sensitive competitive pressures and limited-time needed for employees with unique combinations of technical and security skills, business skills, and hands-on experience has led many employers to pursue "buy" decisions in this labor market, rather than "make" decisions (to hire, then subsidize training in information security). Thus while there is a need to address the growing demand for highly skilled IS workers, there is the additional challenge of meeting the unique demands of this rapidly expanding labor market.

What Occupations Comprise the Core IS Work Force?

For our purposes, I have defined the IS professionals' core as computer scientists (including database administrators, computer support specialists, and all other computer scientists), computer engineers, systems analysts, and computer programmers. The core IS occupations are differentiated, generally, from IT-related jobs by significantly higher skill and additional educational requirements in legal and policy issues, ethics, physical and administrative security, and personnel security, to name a few.

The Vital Role of Information Security in a Nation's Economy

The sweep of digital technologies and the transformation to a knowledge-based economy have created robust demand for workers highly skilled in the development, management and use of information security and the

(Continued, Page 7)

(Continued from Page 6)
inherent technology. While there has been explosive employment growth in the software industry for more than a decade, the demand for workers who can create, apply and use information security and the technologies goes beyond the IT industry, cutting across manufacturing and services, transportation, healthcare, education and government. Information technology (IT) is the most important enabling technology in the world today and it must be protected. It is responsible for new products and services; creating new companies and industries; revitalizing existing products, services, and industries; providing new venues for commerce; enhancing our ability to manage information and to innovate; and improving our productivity, quality of life, and national standards of living. IT is changing the way we live and work, and transforming the economies of the worlds' nations at a fundamental level. As a result, IS is entwined with IT at every level of a nation's national infrastructures.

The Business Environment and Its Impact on the IS Labor Market

Today, the business environment for IT product and service producers is having a significant effect on employer approaches to the recruitment, retention, and training of highly skilled IS and IT workers. Today, the computer and data processing services industry is, by far, the largest employer of highly skilled core IS and IT workers, employing more than a quarter of all workers in these professions; in 2006, the industry's share is projected to rise to nearly 40 percent. While product and technology life cycles have decreased markedly across all industry sectors, time pressures are most intense for these IT product and service producers and the IS professional. These companies confront life cycles or project deadlines that are measured in months or Internet years (when a couple of months are equal to a year). Keeping pace is critical.

In industry segments characterized by fast-paced creators or innovators of IT products and services, jobs and companies change rapidly, with a high rate of creative destruction. In this group, a few firms will grow into large dominating competitors, requiring an ever-expanding pool of highly skilled IS workers to protect the corporate "family jewels." Other firms will acquire some. Many will die in the creative destruction process.

It is important to note that the development of software is highly labor-intensive. A principal way to accelerate software development is to devote more human resources to the process. In addition, rapid technological change makes it more difficult for companies to predict future resource requirements, in all areas, and introduces greater uncertainty into the business environment. Therefore, companies may not be able to ascertain their specific skill needs very far into the future for both the IT and IS professional. This limiting aspect will have a profoundly negative effect on both the short term training and the long term education of IS workers. ❖

Federal Energy Regulatory Commission to Ensure Protection of Critical Energy Infrastructure Information

The Federal Energy Regulatory Commission (FERC) recently finalized a plan to protect the American public by safeguarding certain information about the nation's energy infrastructure. Within a month of the terrorist attacks of September 11, 2001, the Commission began a public proceeding to examine its critical energy infrastructure information (CEII) policies.

The final rule for the most part generally follows the outline of a Notice of Proposed Rulemaking (NOPR) issued last September and continues current practice. It defines CEII and establishes a timely procedure for the public to request and obtain such information, which encompasses only a very small portion of information available from the Commission.

To qualify as CEII, information must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act (FOIA). Information that identifies the location of infrastructure is not considered to be CEII.

A new position of Critical Energy Infrastructure Coordinator will be created to efficiently process non-FOIA requests for CEII.
(Continued, Page 9)

The Strategic Petroleum Reserve: A Critical National Asset

The Strategic Petroleum Reserve (SPR) is the nation's first line of defense against disruptions in world petroleum supplies. It is an emergency supply of crude oil stored in huge underground salt caverns along the coastline of the Gulf of Mexico. The SPR significantly reduces our nation's vulnerability to the adverse economic, national security, and foreign policy ramifications of unforeseen petroleum supply interruptions.

Currently, the SPR has a capacity of over 600 million barrels of oil. Its sheer size makes the SPR a significant deterrent to any oil export cutoffs and a powerful tool of American foreign policy. The oil producing countries of the world know the U.S. government has the capability to make up for a certain amount of petroleum shortfalls at any time, and must take this into account when calculating any changes to their oil production and distribution schemes.

The SPR is the largest emergency supply of oil in the world. As a national investment, the crude oil housed in the SPR and the infrastructure supporting it are valued at over $20 billion.

Decisions to withdraw crude oil from the SPR during an energy emergency are made by the President under the authority of the Energy Policy and Conservation Act. In the event of such an emergency, SPR oil is distributed by competitive sale.

Only one time in history has the White House made the decision to tap into this critical American stockpile: during Operation Desert Storm in 1991. At that time, the SPR more than proved its value to U.S. national security. The Department of Energy implemented a drawdown plan to sell 33.75 million barrels of crude oil, the terms of which were agreed to by the International Energy Agency.

The event which proved to be the real watershed in regard to American oil policy, however, was the 1973-74 Arab oil embargo.

Due in part to the existence of this "insurance" against a disruption in oil supply, world oil prices remained relatively stable. In the end, the White House was able to make the decision to release only about half of the original amount allocated, or around 17 million barrels.

The Desert Storm drawdown, and the resultant price stability in world markets that followed, showed the merits of this powerful new tool in the hands of U.S. foreign policy administrators. Washington in effect had announced its willingness to draw upon its emergency supply very early during a time of international crisis, and the plan worked.

The idea to create an emergency supply of oil within the United States is not new, however. A recognition of the need to create a national oil storage reserve has been acknowledged for almost six decades. Interior Secretary Harold Ickes advocated the stockpiling of emergency crude oil as early as 1944. Presidents Truman and Eisenhower both agreed, especially in the aftermath of the 1956 Suez Crisis, a conflict that was precipitated in part by the wave of nationalizations that took place in the immediate post-colonial period.

The event which proved to be the real watershed in regard to American oil policy, however, was the 1973-74 Arab oil embargo. Once again, an upheaval in world politics (this time the latest in a series of Arab-Israeli wars) sent major economic shockwaves throughout the country.

In the aftermath of the oil embargo, the White House made the historic decision to do all it could to protect our nation's access to this vital resource: it created the Strategic Petroleum Reserve. On July 21, 1977, the first shipment of oil - 412,000 barrels of Saudi Arabian light crude - was delivered to the U.S. government for this purpose. The fill of the Nation's emergency oil reserve had officially begun.

The Gulf of Mexico was chosen as the home of the SPR because of its ideal geologic makeup (SPR

(Continued, Page 11)

(Continued from Page 7)
The Commission said it would release project location information needed by parties participating in the National Environmental Policy Act (NEPA) process, while protecting more detailed information not typically needed by those participating in the NEPA process. The rule gives specific examples of protected and unprotected information.

The final rule defines critical infrastructure as "existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters." It includes proposed and existing systems.

Prior to this action, the Commission issued a policy statement on CEII on October 11, 2001, which addressed the issue of removing certain documents from the public domain. On January 16, 2002, the Commission issued a Notice of Inquiry (NOI) setting forth the Commission's views on how it intended to treat previously public documents, and asked the public to comment on specific questions related to the removal of such documents. On September 5, 2002, the Commission issued the NOPR which took into account the comments from the NOI and revised the policy statement to include as CEII information on proposed facilities and exclude information regarding location of facilities.❖

National Petroleum Council

The National Petroleum Council (NPC), a federally chartered and privately funded advisory committee, was established by the Secretary of the Interior in 1946 at the request of President Harry S. Truman. In 1977, the U.S. Department of Energy was established and the NPC's functions were transferred to the new Department. The purpose of the NPC is solely to represent the views of the oil and natural gas industries in advising, informing, and making recommendations to the Secretary of Energy with respect to any matter relating to oil and natural gas, or to the oil and gas industries submitted to it or approved by the Secretary. The NPC does not concern itself with trade practices, nor does it engage in any of the usual trade association activities.

The NPC is chartered by the Secretary of Energy, under the provisions of the Federal Advisory Committee Act of 1972. The Council membership of approximately 175 persons is selected and appointed by the Secretary of Energy. Individual members serve without compensation as representatives of their industry or associated interests as a whole, not as representatives of their particular companies or affiliations.

The advice of the NPC is transmitted to the Secretary in the form of reports approved by the Council and is rendered to the government as a public service. The cost of providing this service is borne by voluntary contributions from the Council members. The NPC conducts studies in response to specific requests originating from or approved by the Secretary of Energy. The Council does, however, reserve the right to decline to undertake any study requested of it by the Secretary, if it determines the subject matter to be inappropriate for Council consideration. ❖

The origin of the National Petroleum Council stems from the experience of government/industry cooperation during World War II. The importance of petroleum to the war effort was cited by President Roosevelt in appointing Secretary of the Interior Harold L. Ickes as Petroleum Coordinator for Defense. Secretary Ickes in turn recognized the value of industry advice in the development of petroleum policies and appointed the Petroleum Industry War Council, whose charge was to:
...mobilize most effectively all resources and abilities of the petroleum industry to deal with the emergency conditions under which the industry must operate, and to provide a competent, responsible and representative body.
In May 1946, President Truman stated in a letter to the Secretary of the Interior that he had been impressed by the contribution made through industry/government cooperation to the success of the World War II petroleum program. He felt that it would be beneficial if this close relationship were to be continued and suggested that the Secretary of the Interior establish an industry organization to advise the Secretary on oil and natural gas matters. On June 18, 1946, the Secretary of the Interior established the National Petroleum Council as the peacetime successor to the Petroleum Industry War Council.

Critical Infrastructure Protection: Legal Questions at the Forefront of National Security
A conference sponsored by the CIP Project of the National Center for Technology and Law,
GMU School of Law
May 9, 2003

This one-day conference will feature leading academics and practitioners addressing the following legal issues:

- Where and how can the United States prosecute terrorists?
- Cybersecurity and Self-Help: How much is enough?
- Parameters on Government Reaction: Protecting the First Amendment, the Right of Privacy, and Posse Comitatus in an era of fear.

For more information on the conference, contact Emily Frye at ffrye@gmu.edu or (703) 993-4170.

Links to Oil and Natural Gas Organizations

American Gas Association	http://www.aga.org/
American Petroleum Institute	http://www.api.org
American Public Gas Association	http://www.apga.org/
Energy ISAC	http://energyisac.com/
Federal Energy Regulatory Commission	http://www.ferc.gov/
Fossil Energy (US DOE)	http://www.fe.doe.gov/
Gas Processors Association	http://www.gasprocessors.com/
Independent Petroleum Association of America	http://www.ipaa.org/default.asp
International Association of Oil and Gas Producers	http://www.ogp.org.uk/index.html
Interstate Natural Gas Association of America	http://www.ingaa.org/main/index.php?page=main
National Association of State Energy Officials	http://www.naseo.org/
National Petroleum Council	http://www.npc.org/
NPC Report (2001): Securing Oil and Natural Gas Infrastructure in the New Economy	http://www.fe.doe.gov/oil_gas/npc/cipstudy/index.shtml
Office of Pipeline Security	http://ops.dot.gov/
Strategic Petroleum Reserve	http://www.spr.doe.gov/

(Continued from Page 2)
refineries and pipelines.

Computer security has the same priority as the physical protection of refineries or pipelines. Specialists have been installing firewalls and improving password systems to make technologies invulnerable to attack. The Department of Energy, with industry support and cooperation, has conducted over 100 vulnerability surveys at key energy assets since January 2002, and has conducted cyber-attack vulnerability testing. DOE has committed to industry to protect the information gained by these assessments as national security information. Activities are also underway for an oil sector system-wide assessment on the West Coast.

API has also forged a partnership with the FBI and other law enforcement agencies to make sure that information about terrorist threats are quickly conveyed to those who need to know about the possibility of attack. This includes weekly telephone conference calls with the FBI and frequent meetings among company security professionals and federal officials.

Over the last several months, API has rapidly delivered several warnings from U.S. intelligence and law enforcement sources through a secure communications network to companies whose facilities are potential targets. API has also merged some of its responsibilities for relaying security alerts with the Energy Information Sharing and Analysis Center.

In order to help oil and natural gas companies better evaluate and respond appropriately to security threats, API has developed a series of regional security workshops. The seminars include a panel of federal agencies with oversight of the industry, including the U.S. Coast Guard, DOI's Minerals Management Service, DOE's Office of Energy Assurance, DOT's Office of Pipeline Safety, the Transportation Security Administration, and IAIP Directorate of the DHS. The next workshop, the Industry Security Seminar and Security Vulnerability Workshop is April 23-25 in Houston, Texas.

We got a dramatic wakeup call on September 11. But we have also moved very rapidly on our own to protect the industry and make sure there is no disruption in the flow of energy to American consumers and businesses.

Kendra Martin heads the security team at the American Petroleum Institute and is the director of E-Business at API. She can be reached at 202-682-8517 or martink@api.org. ❖

(Continued from Page 8)
oil is placed in hundreds of natural salt domes concentrated along the coast), and because it is located near many U.S. oil refineries and the distribution points for tankers, barges and pipelines.

Today, the primary objective of SPR managers is to maintain the readiness of our national oil stockpile for emergency use at the President's direction.

During the 1990's, SPR infrastructure was upgraded to ensure its continued readiness through the year 2025. Pumps, pipes and other key components of the Gulf Coast sites were refurbished or replaced altogether. This effort was extremely successful. It was completed in March 2000, on schedule, and below cost. The SPR will continue to provide the United States with enhanced access to one of our nation's most vital natural resources, and one of the most important elements of our national critical infrastructure, for years to come.❖

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas.