WRITTEN STATEMENT OF

JOHN CHAMBERLAIN

Security Manager Asset Protection Services
Corporate Security, Shell Oil Company

On behalf of Shell Oil Company and the American Petroleum Institute

Before the

SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL OPERATIONS

Hearing on "Chemical Facility Security: What Is the Appropriate Federal Role?"

July 27, 2005

Senate Dirksen Office Building, Room 562, 10:00 AM

Chairman Collins, Ranking Member Lieberman and Members of the Committee: My name is John Chamberlain and I am a manager within Corporate Security for the Shell Oil Company. I also serve as Vice Chairman of the Security Committee for the American Petroleum Institute. I have many years of experience working with Shell's refineries, chemical plants, and distribution terminals. I also have 30 years of law enforcement experience.

I am pleased to appear before you today to testify on the issue of chemical security, representing Shell Oil and the American Petroleum Institute (API). Shell Oil Company is an affiliate of the Shell Group, a global group of energy and petrochemical companies, operating in more than 140 countries and territories, employing more than 112,000 people. Approximately 24,000 Shell employees are based in the U.S. Shell Oil Company, including its consolidated companies and its share in equity companies, is one of America's leading oil and natural gas producers, natural gas marketers, gasoline marketers and petrochemical manufacturers. API is the national trade association for the U.S. oil and natural gas industry, represents all sectors of the industry, including exploration, transportation, refining, storage, distribution and marketing.

The U.S. oil and natural gas industry is committed to protecting the reliable supply network of fuels and products to keep our economy growing. The industry has long operated globally, often in unstable regions overseas where security is an integral part of providing for the world's energy needs. Although we are in the energy business, some proposals to address the security of chemical sites could have affected the energy industry, as well as agriculture, water treatment, food and dairy processing, pharmaceuticals, bulk storage terminals, and small businesses. These U.S. industries are essential for our national security and economic vitality, but not traditionally thought of as "chemical industry" facilities.

My testimony today will first outline the three stages of addressing industrial security: finding vulnerabilities, enacting countermeasures and sharing intelligence. While it is rarely reported on, the industry in partnership with the government has taken many actions to improve industrial security. We have operated under federal security law, federal security partnerships, industrial security practices and intelligence sharing and support these ongoing efforts.

Oil, natural gas and chemical plant operations are now safer and more secure as a result of the public-private partnerships and numerous new federal security requirements. Little has been communicated about the actions that Congress, industry, government agencies, and state and local first responders have taken, but these public-private partnerships and new security laws have improved security to ensure the reliable flow of energy to consumers.

Since we support continued security enhancements, my testimony will then address specific proposals that we believe would be disruptive to our industrial security operations. Congress has been wise to avoid passing environmental mandates and public release of security information proposed in the name of protecting the industry from terrorist attacks. These would be disruptive to ongoing security operations.

We hope that you would avoid provisions that would be counterproductive to the gains we have made in security since 9-11. Whether or not new security legislation is passed, we will continue, in partnership with the government, to re-evaluate and improve security in U.S. oil and gas operations. Our oil and gas infrastructure is the most reliable in the world and our aim is to continue our coordinated efforts to enhance our infrastructure security.

The U.S. oil and natural gas industry has long operated globally, often in unstable regions overseas where security is an integral part of providing for the world's energy needs. After September 11th, 2001, the industry partnered with federal and local authorities to reevaluate and strengthen our domestic security. The world of corporate security changed forever on 9/11, as we had to more seriously address the possibility of intentional acts to harm our facilities and employees instead of just accidental events.

Within months of the attack, the industry developed security measures for all segments of the oil and gas network – including pipelines, refineries, terminals, and others. One reason the industry was able to move so quickly is that we have high caliber security professionals working for companies who are experts in physical security and protecting our assets. At Shell, our corporate security staff has extensive background in federal, state or local law enforcement as well as experience in military security.

Nationwide, oil and gas companies made major investments in hardening facility protection, training and communications all the way from wellheads and offshore platforms to tankers, ports, pipelines, refineries, storage tanks, and most importantly, employees, our contractors and their communities.

All of these steps were carried out in close partnerships with federal, state and local law enforcement and security officials. The partnership forged between the oil and natural gas industry and government at all levels is now working to protect hundreds of facilities across the country from the potential of terrorist attacks. With this history in mind, we ask that you recognize these efforts and avoid disrupting them as you consider if new proposals to improve the security of U.S. refineries and chemical plants are needed. A terrorist, unlike a pollutant or physical workplace, is clever and has the ability to adapt against a checklist of rules. This is one reason we value our close, professional partnerships of the government, industry and local communities in addition to security requirements.

Some legislators may be tempted to treat security as a concern to be addressed with inflexible regulations. We ask that you recognize that a terrorist, unlike a pollutant or physical workplace environment, is clever and has the ability to adapt against a checklist of rules. This is one reason we value our close, professional partnerships of the government, industry and local communities.

Three steps: Find Vulnerabilities, Enact Countermeasures and Communicate Threats

At every stage, we have been mindful that we are protecting not only our facilities and our petroleum products, but also the people who work for Shell Oil Co., our on-site contractors and the neighboring communities. This reassessment of facility security since 9/11 has been a three-stage process: (1) reevaluate our threats and vulnerabilities, (2) carefully put security standards and countermeasures into place and (3) improve systems for communication with federal, state and local law enforcement about terrorist threats quickly.

API and the National Petrochemical and Refiners Association produced an industry-wide method for managers to identify security vulnerabilities in their operations. The SVA methodology is a sophisticated, risk-based tool used to identify the security hazards, threats and vulnerabilities of a facility, and to evaluate the best measures to provide safe facility operations to protect employees and surrounding communities. In other words, it provides the framework for a complete security analysis of the facility and its operations.

The SVA covers both physical and cyber security, process safety, facility and process design and operations, emergency response, management and law enforcement.

In 2004, the oil and natural gas industry expanded the SVA methodology to include to pipeline, truck, rail and liquefied natural gas (LNG) operations. DHS has recognized the SVA methodology and even uses it to train its own employees.

API and federal security personnel also completed the "Security Guidelines for the Petroleum Industry," to help managers protect facilities and respond to changes in the threat level. This guidance is now in routine use as a roadmap for companies in deciding how best to protect all sectors of the industry against the threat of attack. These are the working methods and countermeasures the oil sector uses to protect all segments of the industry.

The guidelines are important because they allow companies to effectively manage security risks and provide a reference to federal security laws and regulations that have an impact on petroleum operations. The Secretary of Energy and later the Undersecretary for the Department of Homeland Security have endorsed the industry guidelines. These security protocols are constantly being updated and improved. A third edition was published in April 2005.

I am submitting the API Security Guidelines and the API/NPRA Security Vulnerability Assessment to be made part of the hearing record.

To sort out and streamline communications from law enforcement agencies to the industry, API and DOE founded the "Energy ISAC", or Energy Information Sharing and Analysis Center. The Energy-ISAC is an Internet-based, secure, early warning system for making sure that threats and suspicious behavior are relayed between oil and gas operators and homeland security agencies.

The Department of Homeland Security is updating this intelligence sharing system with the Homeland Security Information Network. Along with other companies, Shell is participating in the HSIN, which links owners and operators with each other and with DHS and the intelligence community to permit secure conversations about physical and cyber threats, incidents, vulnerabilities and best practices.

Industry-led actions

Over the last four years, the Department of Homeland Security has assumed primary responsibility for the security of domestic infrastructure. Both the federal Energy and Transportation Departments also have key roles for guaranteeing energy assurance and transport of hazardous materials.

In that time, government inspectors have examined refineries and other key energy production assets and conducted cyber-attack vulnerability tests on critical oil and gas facilities. On the West Coast, DOE and DHS conducted an oil sector system-wide assessment on counter terrorism measures.

Shell has also participated in dozens of industry workshops and training to establish common practices within the company so every sector adopts the strongest possible plan for self-protection.

Like other integrated oil companies, we have joined with DHS in developing a common system for comparing security risks across the nation's varied critical infrastructure. The system, called Risk Assessment Methodology for Critical Asset Protection, (RAMCAP) will give Congress and the Executive Branch the tools they need to make decisions and allocate money on security.

Companies like Shell are also working with DHS, state and local governments to protect and secure the areas surrounding our facilities by establishing clearly identified buffer zones. Shell is also a participant in several security information sharing programs. They include the Energy Information Sharing & Analysis Center and the Oil & Natural Gas Sector Homeland Security Coordinating Council.

In addition, Shell has implemented voluntary actions as part of the American Chemistry Council's Responsible Care Security Code, which further enhances security of our chemicals facilities, our communities and our products. The Security Code addresses facility, cyber and transportation security and has been widely recognized by local, state and federal governments as a model for other U.S. industries.

Complying with Post 9-11 Security Laws

The industry has worked hard to meet and exceed new security requirements enacted by the Congress since September 11th. Under the Maritime Transportation Security Act, the U.S. Coast Guard inspects oil tankers, barges, many refineries, chemical plants, and numerous other storage and shipping facilities. API prepared for a new era in the regulation of oil tankers by meeting on multiple occasions with the Coast Guard and DOE. The Coast Guard's Director of Port Security praised API and company efforts that led to no major interruptions in energy supplies to the U.S. as the MTSA regulations were implemented.

Under the new law, refineries and other waterfront facilities in the United States submitted security plans that have been reviewed and approved by the Coast Guard. MTSA also requires companies to designate facility security officers (FSO) who oversee the implementation of their security plans and conduct quarterly drills and an annual exercise to test how well the facility's security plan has been carried out. We believe that overall the new law is working as intended, a view that is shared by the Coast Guard.

Under the Patriot Act, carriers of hazardous materials are subject to background checks and must prepare security plans to protect themselves and their employees. API adopted recommended practices for managers of offshore platforms to prepare for possible terrorist attacks. This practice is to be used as a reference standard for the federal government.

To provide an early warning against potential cyber terrorist attacks against pipeline computer systems, API published new standards for monitoring the movement of oil through pipelines. The standard is called Supervisory Control and Data Acquisition. In the summer of 2004, 19 oil and gas associations created the Oil and Natural Gas Homeland Security Coordination Council to give the government a single point of reference for the industry when it is needed.

Views on new security proposals

You invited me here today to discuss the possibility of new federal legislation to enhance security at refineries and the rest of the energy delivery system. As I mentioned earlier, we support the continued security enhancements that Congress, federal agencies, state and local first responders and industry has put into operation. We would caution that whatever direction the committee decides to take, that you be careful not to disrupt security practices and partnerships that are already in place. Perhaps, the old caution to medical students, "First do no harm," should apply here as well.

We ask that you keep in mind the principle that security requirements should be risk-based and site-specific. In other words, a one-size-fits-all approach will not work and would only provide a roadmap for terrorists to use to determine industry's security countermeasures.

Some legislators may be tempted to treat security as a concern to be addressed with inflexible regulations. We ask that you recognize that a terrorist, unlike a pollutant or physical workplace environment, is clever and has the ability to adapt against a checklist of rules. This is one reason we value our close, professional partnerships of the government, industry and local communities.

MTSA

Should the committee conclude that legislation is needed, we suggest that it not apply to facilities under existing coverage of the MTSA. Anther option for avoiding disruption is to require all facilities in compliance with this law shall be deemed to satisfy the requirements of new security law.

We also suggest that sites that contain areas only partially-covered by MTSA have the option for the entire facility to be covered by MTSA instead of the new law, thus avoiding duplication in regulations at a single facility.

Examining the MTSA security law, I would like to highlight a few characteristics for your consideration. In implementing a broad new security law last year, the U.S. Coast Guard has, overall, done a successful job in implementing security countermeasures without impeding the commerce it protects. This is in large credit to the U.S. Coast Guard's centuries-long experience in protecting onshore and offshore commerce of the U.S., as well as the existing relationships of local stakeholders and respective Captains of the Port. Without this security expertise and these existing relationships of private sector operations, the MTSA would not have been successful.

The MTSA, like all other federal security laws, protected and strengthened our infrastructure, instead of having a federal bureaucracy attempt to redraw or micromanage how private operators function. In other words, it has a risk-based philosophy; the required security protections must meet the risk under which we operate. The security regulations were not an attempt to change the modern environmental and safety regulations with which we comply.

Complying with other security standards

Facilities should be deemed to satisfy the requirements of new security requirements if they operate under a security program in partnership with federal agencies, such as the Pipeline Security Program in the Department of Transportation and the API Security Guidance Program. Facilities should also be deemed to satisfy the requirements of this new law if they comply with other security requirements that are substantially equivalent. DHS should have the discretion to recognize state security law for designating early compliance status.

IST

During discussions about security at refineries, the subject of "inherent safety' has arisen. Inherent safety is a safety strategy whereby substitute chemicals or processes are used to reduce or eliminate hazards. We strongly oppose any mandates for the inherently safer technology because it would be counterproductive to protecting our infrastructure.

Unfortunately, while the concept of inherent safety is well understood, the application of inherent safety in facilities is less understood. For example, there is no agreed upon methodology to measure the effectiveness of inherent safety or inherently safer options. If you can't measure or evaluate inherent safety, it is unreasonable to impose regulations to mandate it. In addition, the complexity of refineries prevents a prescriptive approach to inherent safety - judgments about process safety hazards are best made by process safety experts at each site. We contend that it is more important to manage the overall risk of a facility using risk assessment methodologies.

Infrastructure security laws already passed by Congress, such as last year's Maritime Transportation Security Act and BioTerrorism Act, authorize enforcement of vulnerability assessments and security plans for private facilities, but do not create a new requirement for "IST". No other security law requires IST for good reasons.

First, creating an "Inherently Safer Technology" requirement for American farms and businesses in the name of national security may actually increase risks. For example, reducing the volume of a hazardous chemical stored at a facility may reduce on-site risk but will increase truck, rail, or barge traffic to maintain raw material, thereby potentially increasing overall risk.

Security law covering companies should be risk-based, not seek out the elimination of all risk, which is impossible. Private farms and company facilities that need to use substances will necessarily intensify their security plans - based on the risk level of these substances. This obviates the need for IST.

Under new IST authority, a Government order for changes to materials or processes might very well create new liability should those orders result in accidental or intentional harm.

Inherently safer technology is already incorporated under existing federal requirements for health and safety -- the Occupational Safety and Health Administration's Process Safety Management Program and the Environmental Protection Agency's Risk Management Program. American farms and company facilities will continue to comply with federal, state and local requirements.

Farms and company facilities, through self-interest, consider the safest, most innovative, and cost-effective technologies. However, new government mandates for IST would require bureaucrats and courts to determine the best technologies for businesses. Creating a new "security IST" authority will allow government micromanagement in mandating substitutions of all processes and substances. This would limit operational flexibility and innovation.

Penalties for non-compliance

Enforcement penalties should reflect the view that farmers, owners and operators covered under a new law are meant to be protected from criminals, not treated as criminals for good faith efforts. In other words, DHS should be required to make several attempts to correct the non-compliance before assessing penalties. Penalties for non-compliance should not include prison sentences for owners or operators. Culpability for terrorist acts is addressed in other law. If the enforcement action is to shut down the facility, DHS will consider the effect to national energy reliability before enforcement.

Protection of Information

DHS should withhold and protect from disclosure under the Freedom of Information Act any record related to vulnerability of and threats to critical infrastructure in their possession, or any information derived there from, as long as (1) the provider would not customarily make the record available to the public; and (2) the record is designated and certified by the provider, in the manner specified by DHS, as confidential and not customarily made available to the public. Any employee of DHS that releases such information should be subject to criminal penalties, and where appropriate, disbarment from government employment. In addition from FOIA exemption, additional protections should be made to prevent the leak of vulnerability information, which would provide a "roadmap" for terrorists and other criminals. Such information should be protected from civil discovery except in a lawsuit brought pertaining to the operator's compliance with the security related provisions of these requirements. In the case of an enforcement proceeding, the information in the case should remain classified.

Security clearances for classified information for both government and non-government personnel should be updated to reflect the unified offices within the DHS. Classifications should correspond to these clearances, ensuring a “read what you write” ability by appropriate company employees.

Conclusion

Oil and natural gas operations are now safer and more secure as a result of the public-private partnerships and numerous new federal security requirements. These public-private partnerships and new security laws have strengthened the reliable flow of energy to consumers.

Congress has been wise to avoid passing environmental mandates and public release of security information proposed in the name of protecting the industry from terrorist attacks. These would be disruptive to ongoing security operations. We urge the Committee to carefully consider the effect any new federal law would have upon existing successful laws, programs and practices.

The oil and gas industry is committed to protecting the reliable supply network of fuels and products to keep our economy growing. Our oil and gas infrastructure is the most reliable in the world and our aim is to continue our coordinated efforts to enhance our infrastructure security.