WRITTEN STATEMENT OF

BOB SLAUGHTER

PRESIDENT

NATIONAL PETROCHEMICAL & REFINERS ASSOCIATION (NPRA)

BEFORE THE

SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL OPERATIONS

HEARING ON CHEMICAL FACILITY SECURITY: WHAT IS THE APPROPRIATE FEDERAL ROLE?

July 13, 2005

Introduction

Good morning, Madam Chairwoman, Ranking Member Lieberman, and Members of the Committee. I want to thank the Committee for holding this important hearing today. I look forward to discussing how the refining and petrochemical industries are performing the critical task of maintaining and strengthening the security of our national energy and petrochemical infrastructure. I will also discuss principles for chemical security that we hope the Committee will consider and adopt as it moves forward to develop legislation regarding chemical facility security.

NPRA, the National Petrochemical & Refiners Association, has more than 450 member companies, including virtually all U.S. refiners and petrochemical manufacturers, their suppliers and vendors. Petrochemical companies use manufacturing processes similar to those in a refinery. NPRA companies supply consumers with a wide variety of products used daily in their homes and businesses. These products include gasoline, diesel fuel, home heating oil, jet fuel, lubricants, and the chemicals that serve as building blocks for everything from plastics to clothing, medicine and computers.

Overview/Summary of Statement

Maintaining the security of our facilities has always been a priority at refineries and petrochemical plants. Refiners and petrochemical manufacturers are heavily engaged in maintaining and enhancing security – and were so before September 11. These industries have long operated globally, often in unstable regions overseas where security is an integral part of providing for the world's energy and petrochemical needs. When the tragic events of September 11, 2001, occurred, the nation realized immediately that additional threats had to be taken into consideration in order to protect our homeland. The refining and petrochemical industries drew the same conclusion. Industry – and I say this with special emphasis – did not wait for new government regulations before implementing additional and far-reaching facility security measures to address these new threats.

What are some of the steps our industry has taken to strengthen security? Industry has conducted security vulnerability assessments, prepared and implemented facility security plans, and developed close, working relationships with key federal agencies and state and local law enforcement offices to obtain and exchange information critical to maintaining infrastructure security. Industry has held joint training exercises simulating actual terrorist attacks and developed educational programs involving federal and state government officials with security expertise. Industry personnel from the largest companies to the smallest have shared best practices at NPRA meetings and conferences. With this strong evidence of our commitment to facility security as background, NPRA urges the Committee to consider the following facts:

- The refining and petrochemical industry will continue to maintain and improve our security operations to protect the vital network that provides a reliable supply of fuels and other petroleum and petrochemical products needed to keep our nation strong and our economy growing.

- Industry, in cooperation with government security agencies, has reassessed security vulnerabilities and implemented strong and effective security measures since September 11, 2001.

- Essential working relationships and information networks have been established between government security agencies and the refining and petrochemical industry to exchange "real-time" intelligence data on security issues to allow them to respond rapidly to terrorist threats.

- Industry has partnered with the Department of Homeland Security (DHS) on many important security initiatives and programs, including the Risk Assessment Methodology for Critical Asset Protection, or RAMCAP, the Homeland Security Information Network (HSIN), and Buffer Zone Protection Plans.

- Industry complies with the security requirements under the Maritime Transportation Security Act (MTSA) which is administered by the U.S. Coast Guard. The Coast Guard and industry are working together closely to achieve the security goals of the Act.

- MTSA has been an effective security regulation. It enjoyed broad bipartisan support in Congress. For these reasons, NPRA recommends that the Committee use MTSA as a model as it develops new DHS regulatory authority to address chemical security issues.

- Any new legislation should recognize and give credit to companies for the security programs they have already implemented.

Industry has Conducted Facility Security Vulnerability Assessments

In 2003, NPRA, working with the American Petroleum Institute (API), DHS and the Department of Energy (DOE), developed and provided industry a peer-reviewed security vulnerability assessment (SVA) methodology for our industry. In 2004, industry expanded that methodology to include transportation-related activities, including pipelines and rail and truck transportation. DHS has endorsed the vulnerability assessment methodology and uses it to train its employees.

The security vulnerability assessment methodology is a sophisticated and effective 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 the public. The methodology provides the framework for a complete security analysis of the facility and its operations. Depending on the type and size of the facility, the assessment utilizes expertise in physical and cyber security, process safety, facility and process design and operations, emergency response, management, law enforcement, and other disciplines as necessary.

Differences in geographic location, type of operations, and on-site quantities of hazardous substances all play a role in determining the approach taken. Security vulnerability assessments typically include the following types of activities:

- Analyzing the facility to determine what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;

- Identifying and characterizing potential threats against those facilities and assessing their attractiveness as targets;

- Identifying potential security vulnerabilities that threaten the asset's service or integrity;

- Determining the risk represented by these events or conditions by evaluating the likelihood of a successful event and the consequences if it were to occur; and

- Making specific recommendations for incident mitigation and countermeasures appropriate to the risk level.

Based on the results of the security vulnerability assessment, companies identify appropriate security measures and incorporate them in security plans which are then implemented. Individual facilities have spent many millions of dollars in upgrading their security posture to assess and address risk and other related factors outlined here. A small facility in a remote location may have to spend hundreds of thousand dollars; larger ones, in more populous areas, have spent many millions.

The Maritime Transportation Security Act of 2002 Serves the Nation Well

A majority of the almost 150 refineries and 200 petrochemical manufacturing facilities in the United States are subject to the jurisdiction of the U.S. Coast Guard, and are therefore regulated pursuant to the security requirements of MTSA. (See attached map of U.S. refineries.) The Act requires that these facilities conduct security vulnerability assessments and submit comprehensive security plans to the U.S. Coast Guard. These security plans were submitted by facilities in December 2003. They have been reviewed and approved by the Coast Guard. MTSA also requires companies to designate facility security officers who oversee the implementation of their security plans. This officer is required to conduct drills on a quarterly basis to test elements of the facility's security plan. We understand that the Coast Guard has been pleased with the petroleum and petrochemical industry's implementation of the Act.

Industry has Implemented Strong, New Security Measures since September 11

Media reports sometimes leave the impression that the industry has not taken new security initiatives since September 11. That simply is not true. With the critical information gained from conducting their security vulnerability assessments, facilities have taken the following specific measures to enhance security:

- Reconfigured sites allowing critical assets to be set back from the perimeter.

- Installed sophisticated, state-of-the-art electronic intrusion detection systems around our perimeters and on buildings.

- Implemented card-access controls with new biometric technology readers, such as retina or thumbprint scanners.

- Acquired enhanced security communication systems.

- Shared security response plans with local law enforcement and appropriate federal agencies.

- Conducted drills and exercises to test security and response plans.

- Hired additional security personnel to assist in our security efforts, which are an around the clock, seven days per week priority.

This is just a partial list. A longer list of measures taken by our industry is included as an attachment to this statement, but it, too, is only a partial list of measures already taken as a result of a dynamic process.

Industry is Working with DHS to Improve Risk Assessment

NPRA members are working with DHS on the RAMCAP, or Risk Assessment Methodology for Critical Asset Protection, project. This approach to risk assessment and management will provide a consistent framework for the assessment, reporting and management of terrorism risks across the nation's critical infrastructure and to other key resources. This will be accomplished by developing a common risk-based method for comparing security risks, thereby giving Congress and the executive branch the tools they need to make decisions and allocate resources based on risk. In short, RAMCAP aims to put all infrastructures and key resources, including refineries and petrochemical plants, on a common risk platform.

Industry is Working with DHS to Develop Buffer Zone Protection Plans

Our members are also working with DHS, states, and local officials to protect and secure areas surrounding our facilities, which they neither own nor control, by developing buffer zone protection plans. These plans will identify specific threats and vulnerabilities within the buffer zone, analyze and categorize the level of risk, and recommend corrective measures to local law enforcement to reduce the risk of a terrorist attack.

Industry Participates in Private and Public Information Networks to Enhance Security

As stated earlier, information sharing is a vital part of our industry's security efforts. NPRA members serve on several security-related public and private sector boards and task forces. These include participation on the Boards of the Energy Information Sharing & Analysis Center, or ISAC; the Oil & Natural Gas Sector Homeland Security Coordinating Council; and the Chemical Sector Coordinating

Council. NPRA also serves on a working group of the Homeland Security Advisory Council (HSAC), helping to resolve legal impediments that hinder the submission of private sector information to government officials. NPRA members have also agreed to serve on a working group of the President's National Infrastructure Advisory Council.

One particularly important initiative underway – once again, as a cooperative effort between DHS and industry - is the creation and implementation of the Homeland Security Information Network, or HSIN, for the petroleum and chemical industries. HSIN is an information sharing system facilitated by the DHS in partnership with the critical sector organizations. It links owners and operators with each other and with DHS and FBI to enable collaboration in protecting critical resources and to address physical and cyber threats, vulnerabilities, and incidents, and to share information about potential protective measures and best practices.

Industry Sponsors Educational Programs and Holds Training Exercises with DHS and Other Government Officials to Enhance Security at Facilities

NPRA has established a standing committee on security which has held or co-sponsored more than a dozen national facility security conferences and workshops. The agenda has featured federal and state policymakers, security and counterterrorism experts, and the sharing of best practices to afford participant companies the opportunity to learn which new approaches have worked for others. In February of this year, for example, NPRA conducted an intensive training workshop for persons designated as Facility Security Officers which helped them to better fulfill their responsibilities under MTSA. NPRA has held two training exercises in cooperation with Texas Homeland Security. The exercises were conducted by Texas A&M University's National Emergency Response and Rescue Training Center and Texas Engineering Extension Service. The most recent training exercise, "Safe Horizon," was held in March of this year. This exercise was focused on incident deterrence and prevention of a presumed terrorist attack. These training exercises and educational programs provide information that allows companies to better assess the effectiveness of their own security policies, plans, and procedures, and make modifications as necessary.

Industry Relationships with Federal, State and Local Officials Enhance Facility Security and should not be Impeded

The success of security programs in the refining and petrochemical industries is due in large part to the excellent working relationship industry has established with various federal, state, and local governmental bodies. NPRA and its member companies work with more than a dozen federal agencies, as well as state and local law enforcement agencies and emergency responders throughout the nation to share critical infrastructure information and obtain updates on the latest intelligence concerning terrorist focus and targets. Agencies we work with include the FBI, the Department of Transportation, the Department of Energy, the Department of Defense, the CIA, the Government Accountability Office, and, of course, the Department of Homeland Security and its various components, including the U.S. Secret Service, the Transportation Security Agency, and the U.S. Coast Guard.

Industry's relationship with DHS and other security agencies allows immediate access for both government and industry to rapidly changing information vital to maintaining facility security. Frankly, we are concerned about the impact of new legislation on this cooperative relationship. If DHS becomes an industry regulator through enactment of federal security legislation, the dynamics of the relationship will certainly change and this level of information sharing could be diminished. Our homeland security posture, in other words, could be significantly impacted depending on the content and scope of federal legislation. We ask that you keep these concerns in mind as you develop your proposals.

NPRA does not oppose reasonable chemical security regulation; however, the existing system is working well and care must be taken to do no harm to current efforts in fashioning your ultimate product. Although we do not advocate legislation, we realize that this Committee and DHS have both announced support for new regulatory authority to address chemical security. In response, we have developed some principles that we hope the Committee will consider and adopt in federal legislation.

NPRA's Principles for Chemical Security

Our first principle concerns the general construct of any chemical security legislation or regulation. Given the success of Maritime Transportation Security Act, it is NPRA's strong recommendation that MTSA be used as a model for any new security legislation. MTSA has a proven, successful track record and provides all of the essential tools needed to maintain and strengthen security. A MTSA-type regulatory program would include clear performance-based requirements, security vulnerability assessments, facility security plans, exercises, documentation, reporting procedures, audits, and protection for Sensitive Security Information, or SSI. Such a regulatory program should also provide for self-assessment and auditing, possibly to include a program similar to OSHA's Voluntary Protection Program or EPA's Performance Track.

Federal legislation should continue existing U.S. Coast Guard jurisdiction over facility security, and authorize DHS to promulgate MTSA-type security requirements for chemical facilities not regulated by the Coast Guard. Legislation should avoid overlapping jurisdiction with other federal agencies by giving this federal program preemption over other federal or state programs. In addition, some facilities are only partially covered by MTSA. In these cases, we would suggest that they be given the option of submitting security plans to the Coast Guard where logistically appropriate. Legislation or subsequent regulation should allow this type of "opt in" activity to occur.

As previously mentioned, after 9/11 industry did not wait for new government regulations before implementing enhanced facility security measures. Refiners and petrochemical manufacturers have conducted security vulnerability assessments and adopted facility security plans. Any new legislation should recognize and give credit to these companies for the security programs they have already implemented.

An important part of any facility security plan is making sure that the workforce is trained, qualified, and dependable. If background checks of employees and contract

employees are required, we hope the Committee will direct DHS to define specific criteria for denying workers access to a facility. Companies conducting background checks should also be authorized to access and utilize government resources and databases, as is done now for the financial sector.

Federal legislation should require that DHS develop a risk-based approach to regulating both chemicals and facilities. We would suggest that DHS use Section 112(r) of the Clean Air Act Amendments of 1990 (pertaining to risk management plans) as the starting point to define the chemical sector. DHS should then, by regulation, develop a list of chemicals of interest based on security risk as the qualifier for a chemical site to be regulated. The RAMCAP project will be one tool for DHS to use to assess security risk. DHS should also be given flexibility to set the appropriate chemical thresholds based on risk.

NPRA was encouraged by the core principles for chemical security announced by DHS. Those principles for addressing chemical security are based on risk and provide reasonable, clear, equitable and enforceable security standards, while recognizing investments and progress that companies have made to date. We concur with these principles and look forward to working with both the Committee and DHS as legislation is developed.

Conclusions

To conclude, Madam Chairwoman, refiners and petrochemical manufacturers take very seriously their responsibilities for maintaining and strengthening security at their facilities. Our industry has complied with modernized, post 9-11 federal security requirements. We have utilized expert engineers who understand our facilities better than anyone else to conduct vulnerability assessments and implement new measures to protect against new threats. We have called upon experts throughout all of industry, government agencies, and the security industry to determine the best practices to protect our facilities. And perhaps most importantly, the industry has created an outstanding working relationship with government security agencies to receive rapidly the critical information needed to fight terrorism. This working partnership has been very effective in encouraging the exchange of information to allow the industry to focus on the security threats that exist today and are most relevant. NPRA and its members look forward to continuing this security partnership.

In closing, I urge the Committee to fully consider the impact of federal legislation on existing security programs and practices, to use MTSA as the template for developing new chemical security requirements, and to embrace and support the core principles outlined by DHS at the Committee's June 15th hearing. I will be happy to answer any questions the Committee may have on our testimony.

July 2005

FACILITY SECURITY MEASURES TAKEN BY PETROLEUM REFINERS & PETROCHEMICAL MANUFACTURERS

NPRA, the National Petrochemical & Refiners Association, has more than 450 members, including virtually all U.S. refiners and petrochemical manufacturers. Our members supply consumers with a wide variety of products and services that are used daily in homes and businesses and contribute to the nation's quality of life and security. NPRA is proud of the accomplishments refiners and petrochemical manufacturers have achieved in maintaining and strengthening facility security.

NPRA members report they have conducted comprehensive facility security vulnerability assessments and have identified and evaluated critical assets and infrastructure, such as dock facilities, high value production units, power stations, and other equipment which, if attacked by terrorists, could result in significant off-site consequences. Each individual facility is expected to determine what is most important for that particular facility. With this information, facilities have taken the following kinds of specific measures to enhance security:

Formalized information sharing networks with area businesses and local, state, and federal law enforcement and homeland security (such as membership in the Energy Information Sharing and Analysis Center, or ISAC, and the Homeland Security Information Network, or HSIN).

Shared security response plans with local law enforcement and appropriate federal agencies.

Conducted drills & exercises to test response plans.

Hired security personnel, some of which are used around the clock, seven days per week.

Conducted contractor background checks.

Installed perimeter fencing, ditches, berms, and jersey barriers.

Reconfigured roadways and installed speed devices to delay vehicular movement.

Installed a variety of fence-line intrusion detection devices, to include security lighting and area cameras.

Reconfigured sites, allowing critical assets to be set back from perimeters.

Acquired enhanced security communication systems.

Instituted perimeter patrols and surveillance, conducted by both company personnel and local law enforcement.

Installed electronic intrusion detection on buildings (e.g., infrared, motion detectors, door and window sensors).

Implemented card-access controls, with new technology access readers (e.g., biometrics, retina scan).

Required remote parking for employees or contractors, and contractor/visitor vehicles marked with identification (signs/cones).

Required ID badges to be displayed at all times, and instituted procedures for lost ID card and requiring parking decals.

Adopted shipments/deliveries verification process (e.g., close examination of shipping papers, driver's identity).

Identified restricted areas within facilities.

Monitored railroad traffic to and through facility.

Required all visitors to produce identification.

Restricted visitors from driving within the facility.

Prohibited any unannounced visitors.

Rotated access gates on random basis.

Conducted security officer training.

Installed secure mail handling procedures.

Reported suspicious activities (e.g., photo taking, vehicles parked unusually, aircraft over facility).

Conducted vehicle searches (interior & exterior).

Instituted sophisticated processes for collecting and evaluating intelligence/threat information.

Protected computer infrastructure.

Questions about this document may be directed to Maurice McBride, NPRA Director for Security, 202-457-0480, or mcbride@npra.org.

Location of U.S. Refineries 2005