AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PREVENTING TERRORIST ATTACKS ON AMERICA'S CHEMICAL PLANTS

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 15, 2005

Serial No. 109–20

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

24–604 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania, *Vice Chairman*
CHRISTOPHER SHAYS, Connecticut
PETER T. KING, New York
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
CHRISTOPHER COX, California (Ex Officio)

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi (Ex Officio)

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity 1
The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity 3
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Committee on Homeland Security 4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security 18
The Honorable Mike Rogers, a Representative in Congress From the State of Alabama, and Chairman, Subcommittee on Management, Integration, and Oversight 17
The Honorable Peter A. DeFazio, a Representative in Congress From the State of Oregon 23
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 21
The Honorable Bobby Jindal, a Representative in Congress From the State of Louisiana 19
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island 28
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 29
The Honorable Edward J. Markey, a Representative in Congress From the State of Massachusetts 31
The Honorable Bill Pascrell, Jr., a Representative in Congress From the States of New Jersey 25
The Honorable Stevan Pearce, a Representative in Congress From the State of New Mexico 29

WITNESSES

PANEL I

Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, U.S. Department of Homeland Security:
Oral Statement 5
Prepared Statement 8

PANEL II

Mr. Stephen Bandy, Manager, Corporate Safety & Security, Marathon Ashland Petroleum LLC:
Oral Statement 49
Prepared Statement 51
Mr. Frank J. Cilluffo, Director, Homeland Security Policy Institute, The George Washington University:
Oral Statement 38
Prepared Statement 41

Page

Mr. Sal DePasquale, Security Specialist, CH2M Hill and University of Georgia:
Oral Statement 66
Prepared Statement 69
Mr. Marty Durbin, Managing Director of Security and Operations, American Chemistry Council:
Oral Statement 55
Prepared Statement 57
Mr. Allen Summers, President and CEO, Asmark Inc.:
Oral Statement 63
Prepared Statement 64

PREVENTING TERRORIST ATTACKS ON AMERICA'S CHEMICAL PLANTS

Wednesday, June 15, 2005

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 3:00 p.m., in Room 2118, Rayburn House Office Building, Hon. Dan Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Rogers, Pearce, Jindal, Cox (Ex Officio), Sanchez, Markey, Dicks, DeFazio, Jackson-Lee, Pascrell, Langevin, and Thompson (Ex Officio).

Mr. LUNGREN. The Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cyber-security will come to order. The subcommittee is meeting today to hear testimony on preventing terrorist attacks on America's chemical plants. Welcome to this important hearing. We are meeting today to discuss this terrorist threat posed to America's chemical plants and what is being done to protect them in all levels of government and within the private sector.

This is an issue that has received a great deal of attention in the media and within the halls of Congress with many questionable claims and figures on the numbers of chemical plants that are high risk, how many people these plants can harm and what types and quantities of chemicals present a real threat and what has been done to secure these sites against terrorism. It is impossible and would be reckless to attempt to oversee and legislate on national security issues based on misinformation or misconceptions. Thus, the purpose of today's hearing is to build a common understanding of what the facts about chemical plant security truly are so we can make informed policy judgments about what if any additional legislation may be needed in this area.

To this end, I hope our two panels can answer two main questions: First, what is the universe of chemical facilities that pose a real risk of catastrophic terrorism, and two, within this universe, what is being done to reduce security vulnerabilities and what more needs to be done. The Department of Homeland Security over the past 2 years has worked diligently to identify high risk targets across the Nation. This includes the highest risk chemical plants. DHS has done this by modifying work started by the EPA.

The EPA, for environmental and human safety purposes, requires facilities with certain quantities of certain chemicals to file

risk management plans. It has been reported that based on EPA's data, there are 123 chemical facilities at which accidental release of chemicals could affect 1 million or more people. Based on the same data but using a much more precise methodology for assessing the realistic consequences of a deliberate terrorist attack, DHS has identified those chemical plants which could pose a high risk to surrounding communities. DHS's numbers, generally speaking, are dramatically lower than EPA's. And the GAO has testified that even DHS's numbers generally overstate the consequence of a terrorist attack on such facilities due to some very conservative methodological assumptions.

We cannot get into too much detail in this open session. I am satisfied that the briefing for members that took place yesterday confirmed that the universe of chemical plants that could cause serious injury or death to significant numbers of people is very limited and that the actual consequence numbers are only a small fraction of the more ominous population affected figures we read about in the press and that the risk posed by these sites is not necessarily substantially different than those posed by large office buildings, stadiums, malls and other places where other people routinely gather.

My point is not to underestimate the threat, but where does this threat exist with respect to all other threats. My point is how do we make rational risk assessment across the plane and how do we ensure that we don't err on the side of overhype on one side or underestimating on the other. Indeed, the chances of successfully attacking such other sites may, in fact, be greater than targeting chemical plants due to some unique complexities involved in successfully causing an optimal toxic release from chemical facilities. Another major misrepresentation is that no one has done anything to secure chemical plants since 9/11. As our briefing yesterday confirmed, and I hope our hearing today will demonstrate, nothing could be further from the truth, particularly with respect to the truly high risk facilities.

Days after standing up as a new department, officials from the infrastructure protection division of DHS began visiting many of the higher risk chemical facilities around the Nation. Since then, over the past 2 years, the Department has worked to identify the highest risk facilities and to ensure these sites have completed vulnerability assessments and buffer zone protection plans. The Department also has actively assisted these sites for the implementation of protective measures to reduce vulnerabilities, including perimeter surveillance and detection systems, increased barriers and access controls and enhanced response and mitigation training equipment and capabilities.

It is not a totally rosy picture, but the suggestion that nothing has been done, I think, misleads the public. Likewise, the chemical facilities themselves have made substantial investments in the areas of security with many plants implementing voluntary security standards under ACC's Responsible Care Code and similar programs. Of course, we will always say that more can be done or needs to be done and that will always be true. But the goal is here, as with all homeland security efforts, to prioritize risk reduction rather than risk elimination. We should seek to do what is possible

and do that as effectively as possible. We cannot afford to implement millions of dollars of security upgrades at each and every facility across the United States if we are not prioritizing properly.

We must use the concept of risk-based management to ensure our resources are targeted where they are most needed, not just within the chemical sector, but across all infrastructure sectors. I am not yet convinced that all reasonable security measures have been put into place at all the high risk chemical facilities in the country. I am convinced, however, the best way to accomplish this goal is by not diverting our attention in resources towards low priority sites. I look forward in working with the committee and working with the Department to ensure that our highest risk facilities of whatever kind or type are receiving the level of attention and resources they deserve and that they are implementing risk reduction measures recommended by DHS.

I welcome our witnesses today and I look forward to their testimony. And at this time, I would like to recognize the ranking member from California for any statement she would like to make.

Ms. SANCHEZ. Thank you, Mr. Chairman, and I thank our witnesses for being here today. There are just a few sectors of our critical infrastructure that I think have an incredible impact should there be a large type of attack, and I think chemical plants certainly fit in one of those sectors. In a report that was issued by the EPA in 2003, they said that there were 123 chemical facilities throughout the United States that they called toxic worst scenarios, where one million people would be in a vulnerable zone and at risk of exposure to a toxic gas cloud.

The DHS estimates have been done in a different way and the estimates of the number of people that would be killed or seriously injured is two or three orders of the magnitude lower than the EPA numbers. So I know you can't be very specific today, but I would hope that you might try to describe a little what you think is the difference between the EPA and the DHS numbers just so we can try to understand where those differences lie. And I guess the biggest question for me as a Congress person is what role should the government play, because quite frankly, I have sat with a lot of people in industry, particularly the chemical plants and many of them have said to me and I have to prefix this by saying, I am not a real big regulation kind of a person having been in business myself, and having felt completely strangled by some of the red tape and regulation that goes on. But the industry itself, to a large extent, has said to me, if you don't regulate us, the financial incentive would probably be that none of us will go that way, in other words, there are a lot of people in the chemical industry who said put some type of regulation in because it will force all of us to play at the same level.

So I guess we could view it different ways. No regulation, maybe some type of regulation or maybe very heavily regulated. I know, for example, that the nuclear power industry is heavily regulated. And yet when we look at the possible people affected, chemical plants may have a larger magnitude of people they can affect if something could happen and yet there is very little regulation on them.

I just question what is our role with respect to chemical plants. Should we be doing some regulation? Maybe you could shed some light on that. And I guess I would just say that in October of 2002, then Secretary of DHS, Secretary Ridge and EPA administrator at that time Whitman declared, in a joint letter to The Washington Post, that voluntary efforts alone are not sufficient to provide the level of assurance that Americans deserve.

I look forward to your comments and insights about what type of a role the government should play with respect to chemical plants and the industry at large.

Mr. LUNGREN. I thank the gentlelady from California and the Chair would now recognize the chairman of the full committee, the gentleman from California, Mr. Cox, for any statement he might have.

Mr. COX. Thank you, Mr. Chairman. This hearing today, which I congratulate you for convening, reminds us when the Department of Homeland Security was formed by the Congress and began its journey 2 years ago, it was discharging one primary mission from this Congress, to conduct a comprehensive risk assessment of the Nation's critical infrastructure. When this is complete, the next step is to map our Nation's key vulnerabilities against what we know about terrorists' capabilities and intentions. By doing that we can prioritize our protective measures and thereby secure our most critical infrastructure from terrorist attack. That process is well underway, but there is still a great deal more to do.

Since the Department of Homeland Security opened its doors in March of 2003, it has been pursuing an aggressive program to prioritize and address the security vulnerabilities at America's highest risk chemical facilities. To do this, the Department of Homeland Security has used, among other data, EPA data to estimate the worst-case scenarios for potential chemical releases resulting from national terrorist attacks at roughly 15,000 sites across the country. This focus has made sense first because the chemical industry is vitally important to our safety and well-being and to the conduct of our daily lives, not to mention to our economy and to our national security.

And second, it makes sense because the lethality of a handful of chemicals and their proximity to large population centers can make certain chemical facilities highly attractive targets for terrorists. The key is to focus on those chemical plants that do pose a high risk of terrorist attack and on those facilities that would they be attacked, pose a high threat in terms of consequence. DHS and the industry must continue to act aggressively to deal with these risks. We have got to be strategic about homeland security and be guided by the principle of securing the highest risk sites of our Nation's critical infrastructure not only within the chemical sector but elsewhere. This is one of the main themes this committee has pursued that we continuously stress throughout this Congress and the last Congress.

Homeland security resources must be targeted in a risk-based fashion and that targeting has to be based on a continued rigorous examination of threat, vulnerability and consequence. The threat at every chemical plant is not the same. At some, particularly at smaller facilities, the risk is finite and manageable. At others,

there is a high risk to both people and property and to our economy as a whole. We cannot ignore the explicit and bipartisan decision by the Congress in establishing the Department of Homeland Security as we consider how next to pursue this problem of chemical plant security, to withhold from the new Department of Homeland Security regulatory authority directly over critical infrastructure sectors. And so as we conduct these hearings, one of the questions that we are addressing is should we amend the Homeland Security Act to create such explicit regulatory authority.

That bridge once crossed, raises the further question of whether the Department of Homeland Security should have similar regulatory over other infrastructure sectors in the American economy. I want to thank Colonel Bob Stephan from DHS to be here to testify today. We look forward to hearing about what the Department has done to secure the chemical industry thus far and plans for the future. I also want to thank our distinguished second panel of experts. I look forward to their testimony as well. And I yield back the balance of my time. Thank you, Mr. Chairman.

Mr. LUNGREN. I just might say, I have to go to the floor to handle a couple of amendments on the PATRIOT Act. No disrespect to you, I will come back as quickly as possible and the chairman is more than able to handle that. The Chair calls the first panel and recognize Mr. Robert Stephan, the Assistant Secretary of Infrastructure Protection from the Department of Homeland Security, and the Acting Undersecretary for Information Analysis and Infrastructure Protection to testify.

STATEMENT OF ROBERT STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. STEPHAN. Good afternoon, Chairman Cox, Chairman Lungren and Representative Sanchez and distinguished members of the subcommittee. It is my privilege to come before you today on behalf of our Secretary, Michael Chertoff, to discuss the Department of Homeland Security's efforts in collaboration with many others around the Nation to reduce the risk posed to the chemical sector from potential terrorist attack as well as to discuss the way ahead regarding the security of this critical infrastructure sector.

I must begin by saying securing the chemical sector is a very high priority for the Department of Homeland Security. Reducing the risk from terrorism by implementing collaborative security strategies with Federal, State, local and private sector partners to protect the Nation's chemical infrastructure is what this is all about. My discussion with you will include a focus on the risk landscape associated with the sector and the important and cooperative steps that have been taken to close security gaps under the existing voluntary private-public partnership framework.

I note that considerable progress has been made through this voluntary framework and further progress is, in fact, required. As part of Secretary Chertoff's second-stage review of DHS policies, operations and structure, my boss has tasked my team to review the current state of security and ensure we have the proper tools to address threats facing the chemical industry now and in the future. To that end, we are currently assessing the need for a care-

fully measured calibrated risk-based regulatory regime for this sector. To close the existing gaps and reduce the risk across the chemical sector, the Federal Government should adhere to certain core principles regarding any proposed or contemplated regulatory structure. First, we must recognize that not all facilities present the same level of risk across the board and that the most scrutiny from a regulatory regime should be focused on those facilities that, if attacked, could endanger the greatest number of lives, have the greatest economic impact or present other very significant risk.

Second, facilities' security should be based on reasonable, clear, rational, equitable, measurable performance standards. A regulatory framework should include enforceable performance standards based on the types and the severity of potential risks posed by terrorist threats. Facilities should have the flexibility in this scheme to select among appropriate site specific security measures that will effectively address those risks according to various standards.

Third, we should recognize the progress that many reasonable and responsible companies have made to date in security. Many companies have made significant capital investments in security enhancements since 9/11 and we should build upon that very positive progress in constructing the road ahead. The chemical sector, as is the case of all critical sectors of our economy, society and government is a potential target for terrorist attack. While we have, at this time, no specific credible information indicating an immediate threat to the chemical sector, DHS remains concerned about the potential public health and economic harm and consequences should a successful attack be carried out.

The chemical sector consists of widely varied and distributed facilities. The particular vulnerability of any specific facility obviously depends on the type and quantity of chemicals on board a site, the physical layout and locations on a site of sensitive targets and systems, access points, geographic location of the facility and various other variables. Therefore, each facility must have a risk assessment and a security plan tailored to its unique characteristics.

In December of 2003, President Bush issued Homeland Security Presidential Directive Number 7 which assigned DHS the overall responsibility for coordinating a national effort to ensure the security of America's critical infrastructure and key resource sectors. This document additionally requires DHS to develop a sector specific plan for the chemical sector and to work with public and private sector partners to implement necessary protective measures aimed at reducing the vulnerabilities of these critical infrastructure sector and its components.

In line with this guidance, a large number of security visits have been completed and protective measures are being implemented for the highest risk chemical sites in the United States. The Department continues to visit other chemical facilities on a priority basis in coordination with State homeland security officials, emergency managers, State and local law enforcement officials and various individual site owners and operators. DHS and the chemical sector also continue to build a strong partnership based on information sharing and collaboration.

I am pleased to report to this committee that these efforts have yielded a solid information sharing background as well as a comprehensive approach to assessing risk for the first time across the sector. It is important to identify work that the chemical sector has done to date in close partnership with DHS to impact the security dilemma it faces. The owners and operators of this business are voluntarily undertaking a variety of security initiatives. In 2002, the American Chemistry Council developed the Responsible Care Security Code to help chemical companies achieve improvement in security performance through various means, specifically identifying, assessing and addressing vulnerabilities, preventing or mitigating incidents, enhancing training and response capabilities and maintaining and improving relationships with key stakeholders.

A critical component of the Responsible Care Code, in our opinion, is the requirement for an independent third party verification of security enhancements as well as security vulnerability assessment completion. The American Chemistry Council estimates its members have spent more $2 billion following the September 11 attacks through now to deal with the security challenges that they face in their sector.

In closing, at DHS a major focus of the past 2 years has been developing tools for assessing risk and working cooperatively with local jurisdictions and companies to implement appropriate protective measures. As we further assess the status of the chemical sector's largely voluntary security regime, we have also been evaluating whether or not the current scope and level of effort will be sufficient to address remaining gaps as well as emerging threats. In short, while most companies have been very eager to cooperate with the Department, it has become clear that the entirely voluntary efforts and good faith of these companies alone will not sufficiently address security across the entire sector.

Based upon work done to date, we now have greater clarity, in fact, much greater clarity about the tasks that lie ahead, the tested tools we have worked collaboratively with Energy and with industry and a more considerable knowledge base that will help close potential security gaps. By exploring all available means to enhance the existing purely voluntary system, we can ensure all facilities have in place a core base of preparedness, that those facilities that pose the greatest risk are receiving more focused attention, that the Nation's approach to chemical sector security will be based on reasonable, clear, equitable and measurable and enforceable performance standards that reflect the diversity of the chemical sector and its importance to our overall national economy as well as the responsible security investments that its members have made to date.

Since September 11, this Administration has worked in the partnership with stakeholders to enhance the overall security of the very important critical infrastructure sector. Through a combination of sector governance structures, information sharing mechanisms and processes, risk assessment and risk-based planning approaches, programmatic initiatives, law enforcement enhancements and coordination, voluntary industry efforts, the chemical sector has demonstrated considerable progress in bolstering its security

posture across the board, but has recognized that further progress is still required.

By developing a comprehensive risk-based approach for the chemical sector, we expect to be able to bring closure to remaining important security gaps across the facility systems and assets most at risk.

This concludes my prepared remarks and I would be happy to answer any questions that you or the committee have at this time.

[The statement of Mr. Stephan follows:]

PREPARED STATEMENT OF ROBERT STEPHAN

Introduction

Good morning, Chairman Lungren, Representative Sanchez and distinguished members of the Committee. It is my privilege to come before you today to discuss Department of Homeland Security (DHS) efforts to reduce the risk posed to the chemical sector from potential terrorist attack, as well as to discuss the way ahead regarding the security of this critical infrastructure sector.

Security of the chemical sector is vitally important: It is a very high priority for DHS to reduce the risk from terrorism by implementing collaborative security strategies with Federal, State, local, and private sector partners—to protect the nation's chemical infrastructure.

My discussion with you today will include a focus on the risk landscape associated with the chemical sector and important collaborative steps that have been taken to close security gaps under the existing voluntary public-private sector partnership framework. I note that considerable progress has been made through voluntary efforts, but that further progress is required.

As part of his Second Stage Review of DHS policies, operations and structure, Homeland Security Secretary Michael Chertoff tasked his team to review the current state of security and ensure that we have the proper tools to address threats facing the chemical industry, now and in the future. To that end, we are currently assessing the need for a carefully measured, risk-based regulatory regime in this sector.

Today, I can report on his behalf that Secretary Chertoff has concluded that from the regulatory perspective, the existing patchwork of authorities does not permit us to regulate the industry effectively. To close the existing gaps and reduce risk across the chemical sector, the Federal Government should adhere to certain core principles.

First, we must recognize that not all facilities present the same level of risk, and that the most scrutiny should be focused on those that, if attacked, could endanger the greatest number of lives, have the greatest economic impact or present other very significant risks. There are certainly many chemical facilities in the United States that pose relatively low risk. Second, facility security should be based on reasonable, clear, and equitable performance standards. The Department should develop enforceable performance standards based on the types and severity of potential risks posed by terrorists, and facilities should have the flexibility to select among appropriate site-specific security measures that will effectively address those risks. Third, we should recognize the progress many responsible companies have made to date. Many companies have made significant capital investments in security since 9/11 and we should build on that progress.

This testimony will first speak to the nature of chemical sector vulnerability, and then will summarize the significant efforts by DHS and the industry since the September 11th attacks to improve security for the chemical sector. We will, of course, look forward to working with you in the coming weeks on the particulars of proposed legislation.

What Is the Threat to the Chemical Sector?

The chemical sector, as with all critical infrastructure, is potentially a target for terrorist attack. While we have no specific, credible information indicating an immediate threat to the chemical sector, DHS remains concerned about the potential public health and economic harm should an attack occur. The chemical sector consists of widely varied and distributed facilities. The particular vulnerability of any specific facility obviously depends on the type and quantity of chemicals at a site, the physical layout, location of sensitive targets, access points, geographic location, and other variables. Therefore each facility must have a vulnerability assessment—and a security plan—tailored to its unique characteristics.

DHS has identified five areas as the focus of our primary preparedness work with the industry: (1) access and access control; (2) operational security; (3) process control; (4) facility systems operations; and (5) local first responder and external response and recovery coordination. These preparedness planning variables must be refined with reference to potential methods of attack. These include perhaps most importantly: insider threats or sabotage; cyber attack; and attacks using explosives or other weaponry.

DHS has established the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) to develop products to help inform infrastructure owners and operators of any threats they may potentially face, as well as to better inform their security planning and investment decisions.

HITRAC is currently working in partnership with industry to develop an updated threat assessment for the chemical sector detailing plausible terrorist threats on a sector basis. This effort includes available intelligence as well as operational tactics, techniques, and procedures derived from study of overseas terrorist operations.

Federal Government Actions to Reduce Risk in the Chemical Sector

In December 2003, the President issued Homeland Security Presidential Directive 7 (HSPD–7), *Critical Infrastructure Identification, Prioritization, and Protection,* which assigned DHS overall responsibility for coordinating the national effort to ensure the security of America's critical infrastructure and key resource sectors. Additionally, HSPD–7 requires DHS to develop a sector specific plan for the chemical sector and to work with public and private sector partners to implement necessary protective measures aimed at reducing the vulnerabilities of this critical infrastructure. Pursuant to the HSPD–7 guidelines, DHS has worked to improve the security of the chemical sector.

A large number of security visits have been completed and protective measures are being implemented for a number of the highest-consequence chemical sites in the United States—sites that could potentially affect in excess of 50,000 people if attacked. Most of these highest-consequence sites have received numerous visits by DHS technical advisors to assess and improve site security. The Department continues to visit other chemical facilities on a priority basis in coordination with State Homeland Security and Emergency Management officials, State and local law enforcement, and site owners and operators.

Protective Measures Implemented

To date, the Federal government has established the following protective measures programs:

• **Buffer Zone Protection Plans (BZPPs).** BZPPs identify and recommend security measures and local law enforcement coordination for the area surrounding a facility, or "outside the fence," making it more difficult to plan or launch an attack. DHS trains local law enforcement in assessing buffer zone security and validates BZPPs provided by State and local officials. DHS is currently distributing $13.6 million to State and local governments in fiscal year 2005 to develop BZPPs. DHS efforts are intended to:

- Improve the level of deterrence in and around the facility through increased staff and community awareness, increased and more efficient police presence, improved response time and efficiency, etc.
- Improve the probability of detection of an attack in planning or in the early stages of execution, thereby preventing an attack or reducing the likelihood of success.
- Increase the time and logistical support necessary to execute a successful terrorist attack, thereby increasing the likelihood of detection during the planning and preparatory phase.
- Increase the efficacy of both defense and response measures through prior planning and coordination.
- Increase the physical assets available for both defense and emergency response in the event of an attack.

• **Site Assistance Visits (SAVs).** SAVs are essentially "inside-the-fence" vulnerability assessments of critical infrastructure facilities conducted by DHS in conjunction with local law enforcement. SAVs have been conducted at 38 of the highest-consequence chemical facilities. An additional 50 SAVs of high-risk chemical facilities are planned in fiscal year 2006. Sites are subject to SAVs for a variety of reasons, including:

- Determination that the facility is highly consequential, that is, the loss of the facility, for any reason, would have significant national or regional economic and/or public health effects.

- Determination that the facility is of such complexity that an SAV would be beneficial to a subsequent or concurrent BZPP execution.
- Determination that the facility is under threat.
- Request by the owner/operator of a facility that is sufficiently consequential to justify the visit.
- The facility meets the minimum level of consequentiality, combined with the presence of an SAV team in the immediate vicinity, usually performing another SAV in the same community. Such visits are performed as an efficiency measure.
- Proximity to a National Security Special Event.

• **The Maritime Transportation Security Act (MTSA) and Port Security Grants.** Currently, 238 chemical sites fall within the port system as defined by MTSA. Under the MTSA requirements, all 238 of these facilities have been required to: assess their vulnerabilities using an accepted methodology; determine gaps; plan and implement measures to close those gaps; and audit results. These sites also are required to develop and implement detailed security plans, which are audited by the United States. Coast Guard and the owner/operator. DHS' Office of Infrastructure Protection (IP) has worked closely with the Coast Guard to ensure that the MTSA-approved methodology is consistent with the overall IP approach. The effect of this effort has been to establish a baseline level of security at these 238 chemical facilities, against which the Coast Guard can make specific recommendations for enhanced security.

Additionally, over the past four years, 287 Port Security Grants have been issued under MTSA, totaling over $100 million to facilities that include some of the highest-risk chemical facilities nationwide.

• **Facility Security Assessments/Facility Security Plans (FSAs/FSPs).** Under MTSA, owners of chemical facilities located along waterways are required to complete FSAs and FSPs and submit them to the Coast Guard for approval. All chemical facilities subject to MTSA are currently operating with approved FSPs and the Coast Guard has completed on-site compliance inspections to verify these facilities are operating in accordance with their respective FSP. The Coast Guard will visit these and all facilities subject to MTSA annually, at a minimum, to ensure continued compliance.

• **FBI Chemical Sector Outreach Initiative.** The FBI, in coordination with IP, has visited more than 220 chemical facilities for the purposes of conducting terrorism response training, threat briefings, and counterterrorism awareness training.

- **Tabletop exercises.** As part of IP's Exercise Program, tabletop exercises have been conducted at six high-consequence chemical facilities. Additionally, the chemical sector was a participant in Exercise TOPOFF 3, from the corporate level to the individual facility level. The findings from these exercises are compiled in After Action Reports, which serve as a basis for taking corrective actions including upgrading security plans and operating procedures, and planning future exercises.

Increased Information Sharing

Without the active participation of the chemical sector, DHS will not succeed in reducing the vulnerabilities and risks to the chemical critical infrastructure of the United States. DHS and the chemical sector continue to build a strong partnership based on information sharing and active collaboration. A number of new programs have been implemented, including:

- **Chemical Sector Coordinating Council.** Under the National Infrastructure Protection Plan (NIPP), DHS and other Federal agencies are working with sector asset owner/operators to develop protection plans for the chemical sector as well as sector-coordinating mechanisms to ensure collaboration on the identification, prioritization, and coordination of sector critical infrastructure protection programs. This effort also facilitates the sharing of information concerning physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

The Chemical Sector Coordinating Council (SCC) was formed voluntarily by stakeholders within the chemical sector in May 2004, and currently comprises representatives from sixteen key stakeholder associations. The SCC is a single point of contact to facilitate organization and coordination of sector policy development, infrastructure protection planning, and plan implementation activities, including sector-wide planning, development of sector best practices, promulgation of programs and plans, development of requirements for effective information sharing, research and development, and cross-sector coordination.

The Chemical SCC is working closely with the Department to draft the nation's strategic vision for a more secure chemical sector. The Chemical Sector–Specific Plan, which will be completed by November 2005, is a component of the NIPP and will provide a framework for government and private-sector partnership in reducing the overall risk of the sector to terrorist attack.

• **Homeland Security Information Network-Chemical (HSIN-Chemical).** The Chemical SCC also is piloting the Homeland Security Information Network—Chemical (HSIN-Chemical) and will actively participate in the vetting of new HSIN-Chemical users. HSIN-Chemical is a highly secure, two-way information sharing mechanism. It allows private industry users in the chemical sector to receive immediate reports of threats to the sector directly from the Homeland Security Operations Center and our chemical Sector Specialists. Via the creation of online workgroups, industry leaders can collaborate with far flung members of their own company or with security managers from other chemical companies to coordinate response activities and share information. The HSIN-Chemical pilot program completed phase one on June 6, 2005. Phase two will reach beyond the Chemical SCC as we enroll security directors from dozens of large and small chemical companies, while continuing to make refinements to the system. In phase three, HSIN-Chemical will be open to all chemical company employees with a need for access to sensitive security information.

• **Security Guidance to the Private Sector.** Based on data gathered from SAVs and BZPPs, DHS has developed three types of security guidance documents. "Characteristics and Common Vulnerabilities" reports identify the common characteristics and vulnerabilities of chemical sites. "Potential Indicators of Terrorist Activity" reports provide information on how to detect terrorist activity near critical sites. "Protective Measure" reports identify best practices and other protective measures for use at specific critical infrastructure/key resources types. These reports have been distributed to all State Homeland Security Offices, with guidance to share these reports with the owners/operators of critical infrastructure and the law enforcement community within each State, as well as Captains of the Port. The reports are also being distributed via the Sector Coordinating Council structure of the NIPP. I would be happy to share this material with this Committee.

• **National Infrastructure Coordinating Center (NICC).** The National Infrastructure Coordinating Center (NICC) is a 24/7 operations center focused on the Nation's critical infrastructure. It provides industry an immediate point of entry for reporting suspicious incident and threat related information to government. The NICC is a component of the Homeland Security Operations Center, but its mission is to work with industry to both receive and disseminate threat and incident-related information.

• **Sector Specialists.** The Office of Infrastructure Protection has Sector Specialists working closely with both industry and the intelligence community to improve the flow of threat and incident information. The Sector Specialists participate in chemical companies' security exercises and disaster drills; conduct sector outreach; ensure the sector receives necessary threat and intelligence related products; and inform the Department and the intelligence community of the sector's infrastructure protection actions and concerns.

Training

DHS facilitates the provision of various training courses to asset owner/operators, state, local, and tribal governments, and local law enforcement agencies responsible for the protection of chemical facilities. Such courses include: BZPP Workshops; Terrorism Awareness and Prevention Training; Advanced Bomb Technician Training; Surveillance Detection; and First Responder/Preventer Training. DHS facilitates this training through several mechanisms, including using prepared, contractor delivered training programs that have been certified by DHS' Office of State and Local Government Coordination and Preparedness, as well as in-house instruction teams deployed from the Office of Infrastructure Protection, which also delivers DHS-certified training. To date, over 200 participants from the chemical sector have participated in the training courses offered, including tabletop exercises with three major chlorine plants.

Industry Actions to Reduce Risk in the Chemical Sector

It also is important to identify work that the chemical sector has done to date, in close partnership with DHS. The owners and operators in the chemical sector are voluntarily undertaking a variety of security initiatives:

• **Responsible Care Security Code.** In 2002, the American Chemistry Council (ACC) developed the Responsible Care Security Code (RCSC) to help chemical com-

panies achieve continuous improvement in security performance using a risk-based approach to: identify, assess, and address vulnerabilities; prevent or mitigate incidents; enhance training and response capabilities; and maintain and improve relationships with key stakeholders. A component of the RCSC is the requirement for independent third-party verification of security improvements and competent completion of the Security Vulnerability Assessment.

In total, 150 chemical companies belong to the ACC, representing approximately 80–90 percent of U.S. chemical production by capacity. Implementation of the RCSC is mandatory for all ACC members, as well as members of a variety of other chemical sector industry associations, including the Synthetic Organic Chemical Manufacturers Association and the Chlorine Institute.

• **Examples of Specific Actions.** The ACC estimates its members spent $2 billion securing their sites in the 15 months following September 11th and an additional $1.1 billion toward security in 2004. These resources have been used to conduct vulnerability assessments, develop security plans and procedures, and make investments in physical and cyber security improvements for facilities of concern, including: tighter access controls, better surveillance, new process controls and equipment, enhanced crisis management and emergency response procedures, better information/computer security, and more stringent background checks. Similarly, the Chlorine Institute formulated a detailed chlorine-specific security regime that was made mandatory for all of their members.

Reducing Risks in the Chemical Sector

Under the existing voluntary framework that governs the chemical sector, DHS will continue to develop and implement new programs that will allow the Nation to continue to make progress toward reducing risk in America's chemical sector. Programs currently in development include:

• **Risk Analysis and Management for Critical Asset Protection (RAMCAP).** RAMCAP provides chemical sector owners and operators self-assessment tools to assess risk at chemical facilities. RAMCAP data will help DHS to prioritize all chemical facilities of concern in the United States according to relative consequence, vulnerability, and level of threat. Results from RAMCAP assessments will allow comparison of assets from across sectors, allowing for better prioritization of national critical infrastructure protective efforts and resources. The overarching RAMCAP program will substantially improve information included in the National Asset Database, asset prioritization, comparative risk analysis, and owner/operator awareness of the vulnerabilities and consequences at their sites.

• **Consultation & Assistance Program (CAP).** The CAP program is a new initiative being launched in conjunction with several private sector partners, the American Chemistry Council, the Chlorine Institute, and the Synthetic Organic Chemical Manufacturer Association. Under the CAP program, DHS protective security advisors will visit more than 1,000 chemical facilities in fiscal year 2006.

Closing Gaps: The Path Forward

At DHS, a major focus of the past two years has been developing tools for assessing risk and working cooperatively with local jurisdictions and companies to implement appropriate protective measures. As we further assess the status of the chemical sector's largely voluntary security regime, we also have been evaluating whether or not the current scope and level of effort will be sufficient to address remaining gaps and emerging threats. In short, while most companies have been eager to cooperate with the Department, it has become clear that the entirely voluntary efforts of these companies alone will not sufficiently address security for the entire sector. Based upon work done to date, however, we now have greater clarity about the tasks ahead, tested tools and a more considerable knowledge-base that will help close potential security gaps.

By exploring all available means to enhance the existing, purely voluntary system, we can ensure that: (1) all facilities have in place a core base of preparedness; (2) those facilities that pose the greatest threat are receiving the more focused attention that a risk-based regulatory regime will bring; and (3) that the nation's approach to chemical sector security will be based on reasonable, clear, equitable and enforceable performance standards that reflect the diversity of the chemical sector.

Conclusion

The effort to counter the threat and mitigate the risk associated with a terrorist attack on the Nation's chemical sector continues to be one of the Department's most important priorities.

Since September 2001, this Administration has worked in partnership with stakeholders to enhance the overall security of the chemical sector. Through a combina-

tion of sector governance structures, information sharing mechanisms, risk assessment and risk-based planning approaches, programmatic initiatives, local law enforcement enhancements, and voluntary industry efforts, the chemical sector has demonstrated considerable progress in bolstering its aggregate security posture, but further progress is needed. By developing a comprehensive, risk-based plan for the chemical sector we expect to close remaining security gaps in this vitally important area.

This concludes my prepared remarks. I would be happy to answer any questions you may have at this time.

Mr. COX. [Presiding.] Thank you very much for your testimony. I want to pick up where I left off in my opening statement and talk to you about how we can prioritize our efforts in this area and indeed across other infrastructure sectors. Can you describe for the committee the methodology that you use, for example, to compare the number of fatalities that would result from a terrorist attack on a chemical plant on a particular site with the number of fatalities that would result from an attack on a football stadium, at a shopping mall or office building.

Second, to what extent do you take into account the economic consequence and how do you mix those apples and oranges in your analysis in order to prioritize where we place our efforts?

Mr. STEPHAN. For the most part, over the last 2 years, we have had to rely on a more subjective set of criteria than we think is appropriate given the tasks that we were given by the Congress in the Homeland Security Act and by our first boss, Secretary Ridge and now Secretary Chertoff. Recognizing that, we have made considerable investment in terms of time, government employees, resources to crack the code on the risk assessment methodology and analysis process. And I am happy to report that working our way through in priority order first through the nuclear energy sector and now with the chemical sector and shortly to follow many others across the top tier of consequences, vulnerabilities and threats we face, we have worked collaboratively with industry to develop a vulnerability assessment tool known as RAMCAP, at the risk of creating yet another government acronym, Risk Analysis and Management For Critical Asset Protection, again, cooperatively developed between DHS, our industry partners as well as the scientific and lab community of the United States of America.

I think we have cracked the code in technology. It is finally catching up to the tasks that were handed to us by virtue of the Homeland Security Act. Having said that, I think we now have a more scientific way to get at consequences, first and foremost, public health and safety consequences, economic consequences, consequences in terms of national security and defense and so on in terms of the things that homeland security presidential directive number 7 would push us to.

Working through that methodology sector by sector is our plan over the next year or so, but we are now prepared in partnership with industry to roll out this particular vulnerability assessment methodology and its associated Web-based tools across the entire width and breadth of the chemical sector to get to the answers I think you are requiring of me.

Mr. COX. When we are talking about deaths, we are talking about consequence, and it is one kind of consequence and there are economic consequences as well. Off the top, we can discern the dif-

ference between the consequence of killing all of the people at RFK who are watching a baseball game and the consequence of killing an equal number of people if that were possible by then destroying a significant chemical facility because the chemical facility would have an additional consequence, that is a purely economic one that would be more indirect with the loss of a stadium, for example.

So even within the consequence box, which is one of only three we have to be looking at here, there are rather dramatic potential differences across sectors. I am still not clear—let me get one thing straight on the public record if I might. What are we talking about in terms of range of consequence from the smallest chemical facility to the largest chemical facility in terms of potential casualties for human death in terms of consequence? There have been some media reports that have said hundreds of thousands and even millions. My understanding is and I think our ranking member alluded to this as well, it is very different than that. Can you quantify that for us?

Mr. STEPHAN. Yes, sir, absolutely. We use as a base line the EPA's risk management program numbers. What those numbers are intended to produce basically from a safety perspective, a point on the map which represents the epicenter of the facility of concern. They calculate the potential population affected by an accidental—

Mr. COX. I want this more precisely and also watch the clock and let my colleagues ask questions. You are taking the most significant potential loss of life at the most vulnerable chemical facility in the United States of America, what are the casualties in terms of human loss of life that would result in your best estimate?

Mr. STEPHAN. Our best estimate based on the incredible modeling we have done, the highest risk facility in the United States would produce under 10,000 potential fatalities and less than 40,000 people that would demonstrate some effects in terms of anywhere from a near death experience from exposure to inhalation of a toxic chemical to a minor skin blemish caused by irritation through contact with a chemical. Number of orders of magnitude—

Mr. COX. I think I know what we are talking about here, but we plucked from the universe of chemical plants the worst case. Now what is the range? On the low end of the scale, what is the minimum consequence from the least vulnerable plant?

Mr. STEPHAN. Sir,—

Mr. COX. Is it possible to destroy a plant and have nothing in terms of consequence on the human casualty side but for the explosion itself and the casualties you would expect from detonation?

Mr. STEPHAN. Yes, that is correct. Depending on the type of chemical we are talking about, you could have a fire ball on site inside the plant perimeter that may cause casualties among the workforce and the emergency responder force on site, but it would not produce a toxic situation beyond the fence line.

Mr. COX. I think where that leads us rather rapidly and we also know that there is a curve here that is pretty steep and there are a whole lot of these smaller facilities and there are a very few of the big ones that really concern us. It focuses I think rather rapidly on the need to discern one vulnerability from another. If I have a subsequent round and there is time, we might talk about what we

know about terror capabilities and intentions and tactics and how we knit that together with how we might spend our money. I yield my time at this point. I don't see a light, but it has got to be expired. So I yield back my time and recognize the ranking member, the gentlelady from California, Ms. Sanchez for questions.

Ms. SANCHEZ. Thank you, Mr. Chairman. And thank you for being before us. On April 11 of this year, I asked Mr. Chertoff during his appearance before this committee whether he thought that IAIEP needed to have regulatory authority and he answered that in the case of the area of chemical plants, the President had indicated if we didn't get an industry norm for them to do it on their own, that this was an area where you might seek some of that authority.

And in recent news articles I have read, it seems that is where you are headed. I guess, what is the type of authority, regulatory authority would you be looking for? Could you give me some instances what that might look like?

Mr. STEPHAN. In terms of any specific aspects of a regulatory regime, I do not have a set of solutions that have been vetted and approved by Secretary Chertoff and pushed beyond him at this point, but I would like to stress that anything we come up with in terms of regulatory regime has to be risk based and has to lead to a set of performance standards that has built in flexibility to recognize the important work that the private sector has done up to this point yet is enough to close the gaps that remain amongst the critical subset of things that we consider to be high risk in this sector based on threats, vulnerabilities and consequences.

Any type of security regulatory regime has to look at certain general principles or concepts. We have to have an agreed upon accredited methodology for doing risk assessments. We have to build security plans based on those risk assessments. We have to implement protective measures that can be measured in terms of effectiveness. There has to be some kind of auditing function that goes along with all of that. At the end of the day, there has to be a compliance and enforcement mechanism built in. Anything we would seek would have to build in the appropriate combinations of those things in order to be effective.

Ms. SANCHEZ. Over the time that we have had this committee, both as a select committee and as a standing committee, one of my biggest concerns has been that the Department overall, DHS, has, in some—and I characterize this from confused, chaotic, it has been a struggle to merge these 22 different pieces of the government and put them under one label. What do you think is standing up? If we were to give you regulatory authority, don't you think that would be just one more added piece of the puzzle that would be difficult for this Department to absorb and to stand up, given all the problems we have had over the last 2 years?

Mr. STEPHAN. If we are talking about a very sweeping, across-the-board regulatory regime that put an iron clad fist upon the chemical sector, the answer would be yes, but that is not at all what we are proposing here. We are proposing a measured calibrated form of regulatory regime based upon risk, based upon the foundation of the good work that has taken place through other things like the Maritime Transportation Security Act, the work of

the Responsible Care Code industry group. All of those things I think would serve to limit the focus of the request for authority that we would come to you with eventually and hopefully on a very tight time line into the future.

Ms. SANCHEZ. What type of a time line do you think we would have in being able to sit down with you and begin to review what type of authority you might want because certainly this committee would have some say over we would grant that or not?

Mr. STEPHAN. We would like to begin those discussions within the coming weeks.

Ms. SANCHEZ. My other question would be with respect to this whole issue what the EPA say are these 123 catastrophic situations and what DHS has with respect to a smaller amount with respect to in particular loss of life.

Mr. STEPHAN. Sure. There is a difference because they look at it from a safety perspective and we look at it from a security perspective. Inside their cone of people, that might be potentially impacted, every one of those people has to figure into somebody's response plan in terms of the police departments, the fire departments, the HAZMAT guys. Every one of those, say if there is 12 million people inside that cone has to be accounted for, that is the real difference. From a safety perspective, those people have to be built into a rescue and recovery and response operation. And that is fine for the EPA's way of doing business and the missions they have been tasked. For us, we have to drill in on risk and figure out what we think using the best that science can buy us at this time, what are the real number of people within that overall cone of potential impact or effect are going to be fatalities or really going to be casualties based on wind direction, wind speed, meteorological effects at the time of the release. And when you get into the math and science, the numbers come way down from everybody inside this hypothetical circle having some kind of impact based on the release.

Ms. SANCHEZ. I am having a difficult time understanding what the difference is between what the EPA says we need to worry about this pocket of people, even if it is the most outer person that might be somewhat technically affected versus what you just said—this is our answer to let us stop a terrorism attack. What if a terrorism thing does happen and how do we respond to it? We have first responders under the Department of Homeland Security. I guess I am having difficulty understanding what the difference is between how you view it versus what the EPA would view it as.

Mr. STEPHAN. To put into simplest terms I can, our model builds in real effects, meteorological effects, wind effects, so on and so forth, that are going to carry this plume somewhere and actually affect a much smaller percentage of people within that overall circle. The EPA is assuming that the wind can blow from any direction. We don't know what it is going to be at any given day or any given time. So every single person in there isn't necessarily going to be a casualty.

That is what is misleading in the press. Those are not casualty figures. Those are people that might be touched if the wind was blowing in their direction, this great composite universe around this 360-degree circle and every one of those people has to be built

into a safety response plan or protocol. We know the wind is going to blow a certain way at a certain speed and meteorological impacts are going to impact the way that cloud leaves that facility and goes over a populated area. And the wind can't possibly blow 360 degrees across the entire diameter of the circle at any given time. So you are narrowing yourself down in terms of the number of folks we have to worry about from a security perspective.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Mr. COX. Thank the gentlelady. The gentleman from Alabama, the chairman of the Subcommittee on Management, Immigration and Oversight is recognized for five minutes.

Mr. ROGERS. Thank you, Mr. Chairman. I want to follow up on the line of questioning from Ms. Sanchez. And you talked about your anticipation of a proposed regulatory scheme in the not too distant future. And you talked a little bit about how cooperative the relationship has been between DHS and your private sector partners. Do you believe that your private sector partners agree there has to be some regulatory proposals tendered to the Congress?

Mr. STEPHAN. Based upon my discussions with my private sector colleagues, the majority of the folks that are giving voluntary adherence to the Responsible Care Security Code would support some type of regulatory authority given to DHS to help take care of remaining security problems within that sector. The outliers in terms of those that are not members, involuntary adherence to that Code, is a mixed bag, to be quite honest with you, sir.

Mr. ROGERS. You talked in your initial statement about that you have taken several steps between DHS and the private sector to work toward closing these gaps. Can you give us some practical examples of those steps that you have taken?

Mr. STEPHAN. We have done various things. We have set up a sector governance structure. For me, one of the most important things we can do is help gel unity of effort that brings together private, public sector partners to attack a problem. We formed sector coordinating councils that involve Federal departments and agencies, State and local governments as well as the private sector. So we have some leadership across the board looking at this problem. We have set up information sharing mechanisms in cooperation with the private sector. Some they have begun voluntarily on their own. We have pushed our information into those systems. We are working to integrate the chemical sector into our homeland security information sharing network which provides realtime feedback on a Web-based system, kind of an instant messaging approach, able to send them threat information, receiving information back through them, and overall holding security conversations via e-mail in a protected fashion.

That is another example. We have made numerous site visits inside the fences. In the colloquial terms, we have to take a look at vulnerabilities in partnership with them and giving them things to consider in terms of security enhancements. We have worked extensively through our buffer zone protection plan to work with State and local law enforcement officials to make sure they understand what the security posture of the facility itself is and what they are going to be expected to do in terms of a response to pre-

vent or the response to respond to an attack after the fact to make sure they have the equipment, training, protocols down pat and the information connectivity with the private sector owners and operators in those jurisdictions. A lot of collaboration we have pushed building upon, of course, the greater foundation that had been set up by many companies in the private sector.

Mr. ROGERS. I asked that because later in your statement, I was confused as to whether you have developed a sector specific plan for the chemical sector or is it still a work in progress.

Mr. STEPHAN. We have a draft document and it is a work in progress anticipated to be complete in late November of this year.

Mr. ROGERS. And finally, you made reference to the fact that you anticipate there will be the need for third party audits or review of assessments. Who would you envision doing those reviews?

Mr. STEPHAN. Again, the details on that, we do not have these completely fleshed out and I don't have anything that has been cleared by my boss, but we would want to take a look how the system under Responsible Care Code is working, how the system under the Coast Guard's leadership in terms of the MTSA legislation, various ways to do those audits, we want to be able to do them most effectively and most efficiently as we can using the good groundwork that has been laid out already.

Mr. ROGERS. Thank you, Mr. Chairman. I yield back.

Mr. COX. The gentleman from Mississippi, the ranking member of the full committee, Mr. Thompson, is recognized for 5 minutes.

Mr. THOMPSON. Thank you very much, Mr. Chairman. Nice seeing you again. One of the things we have grappled with as a committee is this whole jurisdiction of chemical plant inspection, and I want to kind of limit it to security. At one point, Secretary Ridge and Secretary Whitman indicated jointly that chemical plants should voluntarily work out security plans and they were going to work with them and the Department probably needed to supervise that. Can you tell me, is that still the thinking of the Department or if it is not, where we are at this point?

Mr. STEPHAN. Kind of a confluence of two things is happening. It always has been the administration's position, going back at least 2 years, a voluntarily code is not necessarily going to get us to the point we are going to be able to close all the almost important gaps from a risk-based perspective across the sector. What is different in that position today and why we would like to re-engage with Congress in a partnership to figure out the right solution here in terms of regulatory framework.

Of course, we have been engaged over the past couple of years in several attempts to do just that. What we want to bring to the table this time is a better way to do it, because I think technology is with us. We have now risk assessment tools that have been developed between us and the private sector and we are ready to go so we can, once and for all, have a good agreed-upon methodology that is going to lead us to criticality determination.

The second part of all of this is 2 years ago, the Responsible Care Security Code was just being established, being implemented and getting off the ground. We now know where the limits of that code lie realistically. We did not know that 2 years ago. We are better now in terms of tools, technologies and an actual knowledge base

to come to you in an accelerated amount of time in the near future with a proposed regulatory framework that would be the right framework, no more no less than is absolutely needed we think to close remaining security gaps across the sector.

Mr. THOMPSON. Do I understand now that you see DHS's responsibility is for chemical plant security?

Mr. STEPHAN. Based on Homeland Security Presidential Directive Number 7, the President has given us the overall task of basically coordinating leadership for security in the chemical sector between Federal Government, State and local government and the private sector.

Mr. THOMPSON. When you say coordinating leadership, do you see that as having direct authority for making it happen and supervising that authority?

Mr. STEPHAN. We have authority to make certain things happen on a voluntary basis in terms of putting into effect vulnerability assessment methodologies that we agree are the right thing, but they are voluntarily based. Information sharing networks that are voluntarily based, we do not have a regulatory authority in any way, shape or form, outside of the United States Coast Guard under the MTSA legislation that would force the private sector to enter into any kind of arrangement or cooperative relationship with the government that it does not want to.

Mr. THOMPSON. Do you see at any point in time that you and/or the Secretary might come to this committee or to Congress and ask for that authority?

Mr. STEPHAN. We are proposing at this point in time over the next several weeks in an accelerated manner to figure out the principles we think should guide a measured regulatory framework for the chemical sector and work with you all and your colleagues in the Senate to develop a legislative proposal that would put that into effect.

Mr. THOMPSON. In laymen's terms, are you saying yes or no?

Mr. STEPHAN. I believe I said yes.

Mr. THOMPSON. Thank you very much.

Mr. COX. The ultimate laymen's terms. The gentleman from Louisiana, Mr. Jindal, is recognized for 5 minutes.

Mr. JINDAL. Thank you, Mr. Chairman. I wanted to focus my questions in two different areas. First, I want to get a better understanding of this risk-based regulatory approach. I know it is early and you are coming to us before you have all the specifics in place. I am curious if you could describe how that would work, and specifically, how would a risk-based approach to the chemical industry, how would that compare and evaluate and weight risks with external industries, other soft targets outside the chemical industry? Does the Department intend to adopt this risk-based approach across the entire national infrastructure that it is being asked to protect?

Mr. STEPHAN. The first part of the answer is under Secretary Chertoff's leadership, everything we are doing in the Department of Homeland Security is following a risk-based approach across all of our mission areas, the critical infrastructure protection mission area being one of those. We intend to apply a risk-based approach now with much more sophisticated tools and technology at our fin-

gertips than we had 2 years ago when we began all of this business. So we have a better chance of getting it right and making sure that we put the right kinds of things in place across the board, given the unique circumstances of the individual critical infrastructure sectors that are identified in HSPD–7. So the answer is yes, we want to use a risk-based approach across our critical infrastructure protection mission area.

Mr. JINDAL. Would it be fair to say that a low risk chemical facility may actually be less of a target or less of a risk than a soft target like a shopping center or a sports arena? Would that be a fair comparison?

Mr. STEPHAN. I am not in a position at this point to make that bold a comparison. The risks are going to be based on consequences, which include public health and safety, economic dimensions, psychological dimensions and national security dimensions. They will be coupled with vulnerabilities and with threat assessments to form that critical nexus of criticality, what is critical, what is not. As we use that approach, figure out the right tool based on that approach for each sector ultimately within the next year or so. Because now the technology is with us, we will be able to make those qualitative assessments across the sectors between the apples and oranges that we have not been able to make at this point. Where we are with today's technology is now we can, for the first time, do this with respect to the chemical sector and we intend to deploy that in partnership with the chemical sector in very short order.

Mr. JINDAL. The risk based regulatory regime you are talking about, do you expect it is going to apply across the entire industry or do you think the new regulations will be targeted towards those high risk facilities?

Mr. STEPHAN. We need to target a regulatory regime based upon risk and that means the most high risk facilities. What we have to do now and the heavy work that lays before us is defining the exact criteria, putting a box around what we mean by the chemical sector, first and foremost, defining a threshold above which the regulatory structure would apply. Two key initial steps.

Mr. JINDAL. And the testimony has been helpful. I am trying to understand, I come from a State with a large chemical industry with both low and high risk facilities. And I am trying to imagine a regulatory regime that would be applicable across both ends of that spectrum. One last point of questioning. In your experience up to date with the voluntary efforts with the high risk facilities, have you found the industry and individual facilities to be cooperative? Have they be doing everything the Department has asked? And I don't need a name. Have there instances where they have not been cooperating or not been willing to do what the Department has asked?

Mr. STEPHAN. The general rule of thumb is the industry has been very cooperative. When we go on—here is no facility, for example, that has not allowed us or granted us permission to enter their site and take a look around. The formality of the site assessment visit and the joint vulnerability work we have been able to do with industry has varied from site to site to site as we engaged in this process with them.

So I say it is generally very good, although it is not a 100 percent system that allows me to come back to you and say I think they are doing a very effective job in this facility across the board or these 20 facilities across the board in this risk category. I cannot do that.

Mr. JINDAL. I thank you for your testimony. It is my intent to work with you and it is certainly my desire to protect my constituents at home. We want to make sure we are not vulnerable. At the same time, we want to make sure we maintain the economic viability.

Mr. STEPHAN. We share that goal with you.

Mr. COX. Gentleman's time has expired. The gentleman from Washington, Mr. Dicks, is recognized for 5 minutes.

Mr. DICKS. Mr. Chairman, I appreciated our briefing this morning. And as I look here at the Maritime Transportation Security Act, it says in your testimony, currently, 238 chemical sites fall within the port system as defined by MTSA; that is correct, right?

Mr. STEPHAN. Right.

Mr. DICKS. Under the MTSA requirements all 238 of these facilities have been required to assess the vulnerability under an accepted methodology, determine gaps, plan and implement measures to close those gaps and audit results.

Mr. STEPHAN. Correct.

Mr. DICKS. Now if that is true, then you have got all these other people who don't have to audit results as of now, is that correct?

Mr. STEPHAN. Except those under the Responsible Care Code regime, they do as part of the Care Code, have to do a third party audit. The industry reps later can go into more detail.

Mr. DICKS. There are literally thousands of others that aren't doing that, isn't that correct? Not all high risk, obviously, but there are a lot of other companies who are not doing that, isn't that correct?

Mr. STEPHAN. That is correct and I would defer to the industry reps later to provide you the exact numbers.

Mr. DICKS. What bothers me, if you are near a port or a body of water, you have these very stringent requirements?

Mr. STEPHAN. Correct.

Mr. DICKS. And they have all been implemented? The Coast Guard visits these facilities once a year to make sure they are following through. It seems to me if we have demanded that of these people, it would be only fair to require the rest of them to at least have procedures that are similar to the ones that the MTSA have and it sounds as if you are now going to ask for additional authority in order to do something like that. But what is your comment on that?

Mr. STEPHAN. Simple comment. The MTSA is a geography-based system. If you have a maritime approach, you fall under the regulatory regime that is spearheaded by the U.S. Coast Guard. We think a risk-based approach across the entire sector having to define that threshold is the way to go so we can come to you saying we think things are being effectively and efficiently done in the sector.

Mr. DICKS. This morning we had a discussion, and in that discussion, you said—our assistant said that we had gone out, and as I

understand it, done these buffer zone protection plans for several hundred of these facilities.

Mr. STEPHAN. That is correct.

Mr. DICKS. But in your testimony today, you say that you have only done, in terms of site assistance visits, only 38.

Mr. STEPHAN. Correct.

Mr. DICKS. And you are going to do another 50 this year. That also means as we were told, some of the companies aren't excited to see the Department of Homeland Security come to their doorstep, isn't that right, because if it wasn't that way, wouldn't the number of these site assistance visits be higher and closer to the number where you have buffer zone protection plans, which are apparently worked out with the local community?

Mr. STEPHAN. The inside defense piece, or the site assessment visits statistics that you have there, the buffer zone protection plan involves the Department of Homeland Security working with State and local law enforcement to make sure that they have solid connectivity with the site and that they have focused on prevention preparedness response activities, equipment, things like that, so they can do their job in terms of helping bolster security preparedness of the facility.

Mr. DICKS. I would like to see the site assistance visits number be closer to the buffer zone protection plan, because that would show some cooperation between the companies. I know some of the companies are cooperating. But as you have said, it is uneven. There are some of the other companies maybe who are not part of the group who are not being as forthcoming, isn't that correct?

Mr. STEPHAN. Across the board, I cannot come to you and say it is completely even. But I must also say the great majority of companies are cooperating with us in allowing us site access. Some of them do not allow us to do a complete site vulnerability assessment while we are there. Some of them let us look around, offer some observations and then we move on to the next.

Some of this is also a function of the number of people and the enormous nature of the mission that we have at DHS in terms of the 17 critical sectors, one of which is chemicals. And to the point here, there are pieces of risk that you have to look at across all these sectors. Very importantly a new program we are putting on the books through the help of Congress by giving us additional Federal employees is we are posting now infrastructure protection specialists that work for me in various high threat and industry cluster locations around the United States so that now, I don't have to tie up travel time from a guy from Federal headquarters to go out and help provide site assistance visit or fulfill the site visit assistance requirement. I can put guys on the field now that have more day-to-day connectivity with these folks and I think that is going to close some of the numbers gap that is our responsibility and not industry's.

Mr. DICKS. Let me just ask you this. If in fact under the maritime security program and because some of these people as you mentioned are doing a good job and have voluntarily agreed to do these things, it seems to me that is why the ranking member said, you know, you got to have a level playing field here. You can't let some people off and then have others have to do audits and all this

regulatory thing. It would seem to me that this thing really does cry out for Federal legislation that creates an approach and using a risk-based approach, I completely agree with the chairman on that, but you have to get everybody have the same kind of plan or the ones who aren't doing it are going to have an economic advantage over the companies that are in fact standing up and doing the right thing. They are investing billions of dollars. How can you have part of the industry doing that and another part not coming anywhere near to that? Doesn't this cry out for a Federal kind of solution that creates an overall requirement for all these companies or at least the high risk companies?

Mr. STEPHAN. That is why I am here today to, in your terms, across the high risk components of the chemical sector make sure we have a level playing field. But by level playing field, that doesn't mean the same standards for every single facility across the board in that category. The standards have to be flexible so we can make sure that we are imposing the right regime on facilities based upon risk. So that X amount of security for a facility that on the consequence scale is fairly low and not spending the same amount as someone else that on the consequence part of the scale is very high. We have to achieve a balanced, measured and flexible approach because we don't want to destroy the economic vitality of a very important part of the United States' economy.

Mr. DICKS. There seems to be a significant sector that has been stepping up and putting up money to improve their security and some others aren't. And I think you have to straighten that out. Thank you.

Mr. COX. The gentleman from Oregon, Mr. DeFazio, is recognized for 5 minutes.

Mr. DEFAZIO. Thank you, Mr. Chairman. There is going to be on the subsequent panel a gentleman named Sal DePasquale who is going to testify, a security specialist from the University of Georgia. I want to see if you agree with a couple of principles he lays out. He says without prescriptive standards, there can't be self-regulation. He is criticizing the current regime where it is sort of—the industry out there is sort of freelancing on these issues. And then he says, subsequent security upgrades would require the following and you might comment on this as it would apply to high risk facilities: Construction of formidable property barriers, application of sophisticated intrusion detection systems.

And then as he points out, the best detection system doesn't do much good if you can't have a pretty quick response. And then deployment of a trained and properly equipped security force response to prevent the adversary from reaching the target. And just in commenting on that, I would like to go back to the point you made, you said at the highest risk facility, casualties would be probably under 10,000 with 40,000 affected. And I would like to know of the principles he has laid out here, the security upgrades, are you aware that any of those are in place at this highest risk facility, and do you anticipate those would be the sorts of things you would be looking at in terms of regulation?

Mr. STEPHAN. There is a mixture of human capital investments, technological investments, hardware and fencing type investments that need to be made, and in fact have been made. I am happy to

report that we have had either Coast Guard or DHS IP representatives visit each of the facilities on the top tier of concern in terms of risk. Those types of things are being done. What I want to be able to get to is the point where I can say this is the right solution set for this particular facility and we think it is good to go. Right now, lots of money going out the door and lots of investments taking place and lots of enhancements occurring across the board. I want to be able to come back and look you in the eye and say we think we got it right at this facility.

This was the standard, this was the set of options they chose to put in place against that standard and we are good to go with it and let us move onto the next one. I want that comfort level because the importance of this sector in terms of a critical infrastructure sector merits that kind of face to face between the two of us, and that is what we want to get you.

Mr. DEFAZIO. In thinking about the chairman's comments where he is talking about a stadium full of people and asking about the casualty rates, of course it begs the question of what would one use to kill a stadium full of people effectively versus something that is installed and available for use as a weapon.

In the case of 9/11, the weapons were commercial civilian aircraft loaded with fuel, which means they didn't bring in a weapon, they didn't develop a weapon, they just utilized something that was already available in the commercial sector here in the United States.

And I think that same paradigm would apply to the potential for nuclear plants, most certainly, or chemical facilities; or facilities that aren't necessarily chemical manufacturing plants, but might have toxic chemicals, such as Blue Plains or something in this vicinity with a large concentration of chlorine in there.

Could you comment on that? I mean, to me, it seems that the risk, they will say, "Yes, we want to protect the stadium." But I am not sure what weapon we are talking about that would kill everybody in a stadium, but I do know you talked about essentially an already-installed weapon that could potentially, in a worst case, kill 10,000 people.

Mr. STEPHAN. Well, sir, we are looking diligently across all the 17 critical infrastructure sectors that are defined by HSPD7. There are going to be different solutions for each of those infrastructure sectors based upon the risk landscape associated with each of those sectors.

I think we are coming to you with the appropriate solution for the chemical piece, which is a very challenging problem, but I think there is a solution in sight there. There are other solutions in sight, or that will be in sight, with respect to those other pieces of critical infrastructure in places that bring lots of Americans together on a frequent basis.

So at this point—I don't like the term "apples and oranges," but we are using a systematic approach to walk through these sectors one by one and come back to you with the appropriate solutions in hand, based upon the risk landscape associated with each of these potential target sets.

Mr. DEFAZIO. Okay.

Thank you, Mr. Chairman.

Mr. COX. The gentleman's time has expired.

The gentleman from New Jersey, Mr. Pascrell, is recognized for 5 minutes.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Chairman, more than 3 years have passed since 9/11, and Congress has yet to address the need to secure our Nation's chemical plants. I am glad our committee has finally broken this unconscionable streak and has made this issue a priority.

New Jersey alone has 100 sites where large quantities of highly toxic, highly volatile chemicals are stored and used. Any of these sites have the ability to cause significant numbers of fatalities and serious illnesses within the region as a result of a terrorist attack. The EPA has determined—not the newspapers, the EPA has determined that 11 of these sites—and you know the strip I am talking about, that 2-mile strip in New Jersey, from exit to exit—it could poison more than 1 million people in the event of a catastrophic chemical release. That is what the EPA says. So it goes without saying that it is vitally important that the Congress and the administration finally do something. I am heartened so far that our witness, Assistant Secretary Bob Stephan, seems to agree with that.

Now, the first question I have is, How can we best strike a balance between not giving terrorists specific information about plants or shipments of chemicals, while at the same time ensuring that local emergency officials and first responders are prepared to respond appropriately to an event? That is my first question.

Mr. STEPHAN. Okay, sir. I am not going to validate, to begin with, the numbers. I am not sure that the EPA would agree that a million people would be casualties in the event of an incident in one of those sites. I would defer to the EPA, but I am fairly certain they would not agree with your statement.

Mr. PASCRELL. Excuse me, Mr. Chairman. Are you telling me that I am getting this from the newspaper, and that is not a reflection of what EPA says?

Mr. STEPHAN. No, sir. I am saying that often times what the EPA figures represent are misunderstood. I do not think—

Mr. PASCRELL. Well, we are talking about folks that are going to be poisoned, we are talking about folks that are going to inhale what goes up. We have got 70,000 chemicals in the State of New Jersey, 20 of them are toxic, 20 of them are highly volatile. These are not things that people dream up; and you know it better than I do. I am saying to you—or you are saying to me that I used hyperbole in this?

Mr. STEPHAN. No, sir, not at all.

Mr. PASCRELL. What are you saying?

Mr. STEPHAN. Sir, I am saying that the EPA's statistics are not based on numbers of exact casualties within a circle around a facility, they are based on safety requirements that say on any given day this number of people lies within this circle. The wind is not going to blow or the meteorological effects are not going to facilitate the dispersal of that agent across all of those people inside that circle, that is simply not going to happen, but everyone inside that circle needs to be accounted for in some local jurisdictional emergency response or emergency management plan.

Mr. PASCRELL. We know, Mr. Under Secretary, that weather conditions are going to have a lot to do with what happens. That is not the issue. Would you please answer the question I did ask?

Mr. STEPHAN. Yes, sir, absolutely.

In terms of the safety paradigm, the safety regime under which the EPA operates, I think, has the components that are properly built in that allow the dissemination of information appropriately, some aspects of community awareness—and there are specific statutes that make that a requirement—and even more specific information that is put in the hands of the first responders, police organizations, emergency management organizations, fire fighting organizations so that they have what they need to do planning and to be properly equipped and trained to respond to a safety-related incident at a site.

I think we must be very careful to not take security-related information and put it into that same kind of framework, because the only people that really benefit from that are the folks that are trying to attack us. So I am saying there is a difference between safety information that is mandated through a couple of different laws which—the names, unfortunately, I cannot pronounce, but they give the EPA the authority to do this.

In terms of community awareness programs, State and local preparedness organizations and providing information to the first responder community, I would be dead set against any regime that would allow vulnerability-related information to be put into the hands of terrorist organizations to facilitate their operations they are planning against us.

Mr. PASCRELL. No one is suggesting that, but what I am suggesting, for instance, on a very simple basis is, you ask first responders to be available, you are going to train them. They have every right to know what they are up against; they have every right to know what chemical is there because they fight every chemical fire differently, don't they? They have to know this information. And we hope that there is a very close relationship between what you do, what the fire fighter does, what the police officer does, and what the EPA does.

Now my next question is—

Mr. COX. The gentleman's time has expired. I would ask unanimous consent that the gentleman be given an additional minute because I think we need to finish on one point that I asked about and that you also asked about in your questions.

I just want to make sure that the committee has a clear understanding. So I will let the gentleman proceed.

Mr. PASCRELL. Just quickly—thank you, Mr. Chairman—the EPA has had a long-standing role in monitoring chemical facilities, as you all know. Do you believe that the EPA's expertise warrants a strong role in any future chemical security legislation; and if so, how should that role be structured?

Mr. STEPHAN. Sir, I think that the EPA has appropriately been given the leadership in terms of the safety regulatory framework. I think from a security perspective, the Department of Homeland Security needs to take up that responsibility for such a framework; and we should collaborate very, very closely, as we do—very, very

closely with the EPA in terms of making sure that the safety and the security frameworks are coordinated very, very well together.

Mr. PASCRELL. I have 10 seconds, Mr. Chairman, I just want to ask this quickly.

On the 2-mile stretch that I referred to, on a scale of one to five, what you have seen and what your visitation teams have seen would give us what? Five being the highest amount of security in that stretch, one being the lowest, what is your estimation?

Mr. STEPHAN. The highest risk facilities in that particular stretch are abiding by the Responsible Care Code, and I think they are doing a good job.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. COX. Before we leave this point, I think Mr. Pascrell raised the same question that I raised, and I am not sure that the committee has a clear understanding of what is the answer to the question.

Mr. Pascrell referred to a million people being poisoned. You pushed back a little bit in your response to that. When I asked the same question, the answer that I understood you to give was that in the worst case, based on your modeling and your estimates, the number of casualties would be less than 10,000, and the number of affected people—sickness and so on, which would certainly fit within the definition of poisoning—would be 40,000.

Now, these are big numbers, but when we are trying to quantify risk, there is a big difference between less than 10,000 and 100,000 or a million, so I do think that we need to get on the record the figures that we are talking about.

Mr. STEPHAN. Sir, based on the sophisticated modeling that we have done multiple times over, less than 10,000 fatalities and less than 40,000 people impacted, from a very significant degree down to a very minor degree, as a result of exposure to an agent.

Mr. COX. And my understanding is that the figures that Mr. Pascrell is talking about are also correct figures, but what you are saying is that there are a million, potentially, affected people within this radius, and that, depending on meteorological conditions and so on, the way that this would end up affecting people would limit it to the figures that you provided.

Mr. STEPHAN. That is correct.

Mr. COX. I would yield to the gentleman to make sure that the committee is in agreement about what the testimony is.

Mr. PASCRELL. Mr. Chairman, I do agree, but the fact is, a lot of the mixture of these chemicals, you can have all the models that you want, you can look at the weather conditions as many times as you want, we are talking about very, very highly volatile chemicals. And that is fine, we are in the business, that is an industry in my State and many other States; we want to be helpful to that industry.

I want to know if the industries are helping themselves, Mr. Chairman. And what did they find when they got there? They should not need prodding from the Federal Government. We will assist. We will be partners; we should be, we want to be. We did it with the airlines industry. But there are certain responsibilities that you must have—not you must have, but the chemical industry

must have, and I want to know if they are fulfilling those obligations.

The people who live in New Jersey, and every other place where this happens, have a right to know that as well; don't you think so?

Mr. STEPHAN. Yes, sir, they do. And we believe that the majority of the chemical industry has, in fact, taken prudent, responsible steps to secure their infrastructures.

Mr. PASCRELL. While we don't need hyperbole, we do not need underestimating, because what we do then is let our guard down. And we have another report coming in and another report coming in, and here we are 2, almost 3 years later, we are on this side right now, okay, 3 years later, and we have not had a very specific plan to deal with the problem.

Thank you, Mr. Chairman.

Mr. COX. The gentleman's time has expired.

The gentleman from Rhode Island, Mr. Langevin, is recognized for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. And thank you, Mr. Secretary, for you testimony today. It is obvious, from your testimony and from the questions and answers here today, we all have a lot of work to do, and the sooner we get to it, the better. And we need to complete a risk and vulnerability assessment as quickly as possible.

What I would like to ask, first of all, is, based on actionable intelligence, Where do you place the likelihood of a chemical attack on the priority list? Is it a high-risk, medium- or low-vulnerability likelihood that there would be a chemical attack?

And based again on actionable intelligence, which do you feel is more likely, that terrorists would actually acquire chemicals to use in a terrorist attack, or it is more likely they would attack a chemical facility or processing facility to cause casualties?

Mr. STEPHAN. Sir, you presented the penultimate dilemma of our time. Every day I come to work, my staff and I go through this: What is going to happen next? Where are they going to turn next?

As I said in my testimony, we have no specific credible intelligence at this time that indicates that there is an immediate threat of any kind to the chemical sector, but what we have to do, putting ourselves in the mind of our terrorist adversaries, is take a look in terms of criticality, what the chemical sector represents and what the use of chemical weapons and agents as a weapon means.

I think we are talking about the potential of significant public health and safety consequences, significant economic and financial consequences, psychological consequences and, in certain cases, national security consequences when we are talking about certain facilities that may be the single supplier of a critical chemical product that the Department of Defense and others need to do their jobs.

So I think, given all that, what we know about the Al-Qa'ida organization leads us to the fact that these guys want to try to produce mass casualties, mass effects, mass hysteria. Any type of critical infrastructure that poses the potential for a weapons of mass destruction or a weapons of mass effect kind of consequence

is something that the President has told us to drill down on in HSPD7; and the chemical sector would be one of those things.

Mr. LANGEVIN. In all of those chemical facilities that you are familiar with and that we are looking at right now, what percentage of those facilities have to protect themselves—and maybe the most vulnerable—on their own, without the need for government intervention?

Mr. STEPHAN. I think about—and I will let the spokesman later back me up on this, but somewhere around 80 to 90 percent of the chemical companies by volume capacity are members that have signed up voluntarily to the Responsible Care Code. We think, in the Department of Homeland Security's estimation, about 20 percent or so of the high-risk elements that we are concerned about are not voluntarily signed up to any Responsible Care Security Code and may or may not be taking appropriate precautions, making appropriate investments. There is just no way to determine or gauge the effectiveness of those measures, if they are being taken.

Mr. LANGEVIN. Well, in my opinion, the sooner we can give you the teeth, either a regulation or a law to make sure that they do comply, the better. So I want to thank you for your testimony here today, and I yield back.

Mr. STEPHAN. Thank you, sir.

Mr. COX. The gentleman's time has expired.

The gentlemen from New Mexico, Mr. Pearce, is recognized for 5 minutes.

Mr. PEARCE. Thank you, Mr. Chairman. I am still reading the briefs, and I will pass at this moment. Thank you.

Mr. COX. The gentlelady from Texas, Ms. Jackson-Lee, is recognized for 5 minutes.

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman. I want to thank you and the subcommittee Chair and ranking member of the subcommittee for this hearing that could not be more crucial.

Mr. Stephan, Assistant Secretary, welcome. I am delighted that there is not the word "interim" in front of your name. I understand that you are, in fact, in place, and hopefully, we will have an ongoing relationship.

I wanted to travel sort of the track of Chairman Cox and my good friend and colleague from New Jersey, Mr. Pascrell. First of all, I think it is important to acknowledge—which you have been very fair in doing—that there is such a thing as the Responsible Care Code, the Security Code that a number of members of the industry seem to be participants in or signatories on. Is that correct, sir?

Mr. STEPHAN. That is correct.

Ms. JACKSON-LEE. I think at the same time we need to acknowledge that there are standard reports, such as the U.S. Army report, that says, in any given area if a chemical plant or toxic plant was attacked in a more, if you will, densely populated area, you could eliminate or impact on 2.5 million individuals. That is an existing report, so we need to emphasize the danger of the potential of a terrorist attack on chemical plants which find themselves in a number of areas around the United States.

And I might say I come from a region in Texas that is noted for the chemical industry. We have lived alongside of them for a num-

ber of years, so I think—I wanted to focus on the importance of this hearing and the importance of us being able to work together. So I would like to focus you in this area.

Obviously, without pointing to the intelligence, do you feel there is a cooperative link between the Department of Homeland Security and the chemical industry in terms of sharing intelligence data? Is there a dialogue, an ability to get information quickly to the necessary persons responsible for making decisions in the industry of the respective plants? Do you think that is in place?

Mr. STEPHAN. Yes, ma'am, I think it is absolutely in place, and every day we are actually working to make it better. And as I said, our Homeland Security Information–Sharing Network allows them to pass information to us in terms of strange activities that might be taking place inside their areas of concern, and us to pass national-level threat data to them. The FBI is integrated into this process.

I think we have very timely—in place, overarching systems to get specific information, when it exists, into the hands of owners and operators. In addition to other things like indicators of potential terrorist activities, protected measures, recommendations, we have mechanisms in place, wires and pipes, to pass those things back and forth between us and the industry.

Ms. JACKSON-LEE. And I appreciate that, and I don't think we should take lightly your work which you are now doing, and our work, which is to save lives. And to not take lightly any misstep that we make—either one of us, Congress or the executive—can result in the loss of lives, so the importance of communication is important.

I think it is also important to note that we have entrusted to the airline industry, to a certain extent, trying to improve some of the items that they failed to do after 9/11. Likewise, I want to find sort of that pathway that we can work with in terms of another industry, and this one—for example, I understand a number of companies, as I have said before, or you said, are, in fact, self-regulating or at least adhering to the Care act. One of them happens to be Shell, but you happen to have a percentage of those who are not.

Let me follow up with these final, closing questions:

One, help us help you get on site of those companies that are not complying. I don't like hearing you say they said I could come do a fly-by or a drop-in or drive-by; and then they stop us and say, You are finished. Absolutely not. For the guys that don't want to participate or the guys that are not giving you all the information that you need, absolutely there needs to be an emphasis on getting you where you need to be.

So I want to know what is happening with the ones who are putting a hand up, Stop. And what kind of regulatory authority do you need to deal with the constituency, the population, that refuses to play the game to save lives and to allow you to do the full investigation.

Mr. STEPHAN. What we want to do is, we want to bring those folks on board through a measured, calibrated approach—again, based on risk; and I really need to work out the details and clear them up through by boss in the upcoming several weeks. It has got to be performance based, it has got to allow us to draw a threshold

so that we are not—and a certain amount of companies that represent a very low risk that do not need to be taking sweeping, comprehensive security measures, that they may or may not be doing now.

But then there is another degree of people up here that represent a very high risk, in our perspective, according to our criteria, that do. Many, in fact, are.

We are going to bring a package together, bring to you to work together a package that would delineate exactly the box that we want to draw around this regulatory authority. But it has got to be a measured, calibrated approach, performance based and recognizing the very valued investments that certain companies, and a great majority of companies, have actually made to date.

Ms. JACKSON-LEE. Let me thank you. I am going to want to ask subsequently, in writing, for a list of those that you have approached in the past and you have not been able to view extensively their particular plants; I want the actual names.

The other thing is that I think—I hear you saying that you are trying to get a plan for the regulatory authority. You are asking for some, but you are going to be working with the vast industry to understand the best pathway to save lives; is that my understanding?

Mr. STEPHAN. That is correct.

Ms. JACKSON-LEE. I thank the witness, and I yield back.

Mr. COX. I thank the gentlelady.

The gentleman from Massachusetts, Mr. Markey, is recognized for 5 minutes.

Mr. MARKEY. Can I begin first, Mr. Chairman, with a parliamentary inquiry? And the parliamentary inquiry would go to the question of when a hearing starts.

I arrived here at 10 o'clock this morning, at the appointed time for this hearing. I was then told by the counsel—who is whispering in your rear right now—that the hearing doesn't start until the gavel comes down—

Mr. COX. If the gentleman will yield. The hearing was noticed for 2 o'clock; is that right?

Mr. MARKEY. At 2 o'clock, rather. So I was here at 2 o'clock; and when I arrived, I was told the committee hearing starts when the gavel comes down.

I am now reading the rules of the committee, and it makes no such reference to the gavel coming down, it only makes reference to the point at which—I apologize to you—when the chairman gavels the hearing. I apologize to you.

So I guess what I would say is this: Since I did come over here at 2 o'clock for the hearing to start, but a decision had been made not to start the hearing at 2:00, that the committee then has an obligation to all members to have the staff then call all members to tell them that the member is wasting their time in arriving on time for a prearranged hearing because, first of all, I wasted the 15 minutes coming over here, Mr. Chairman.

And now I have had to wait an hour and a half, even though my intention in arriving at 2 o'clock was to be here on time for a hearing which you had scheduled at 2:00, which then, in the discretion of the Chair, you postponed until later. But it then leaves the mi-

nority with no notice, who has arrived on time, without then having been protected for having arrived at the time that the chairman had scheduled the hearing, but had not yet brought down the gavel, which the counsel tells me is the official beginning of the hearing, not the time that the chairman designated as the beginning of the hearing.

And so, one, I wasted my time coming over for the beginning of the hearing, as it had been scheduled. And two, I am now waiting here, even though I am the third senior on the Democrat side, until all of the other members, who could then be here at a delayed time when the hearing has started, arrived here before me.

So would the chairman announce what the policy is for notifying members as to when the chairman is going to not begin the hearing at the appointed time, so that the members who are adjusting their schedules to be here at that time are given the protection which they are going to need?

Mr. COX. I thank the gentleman for his parliamentary inquiry, and I will respond as follows:

First of all, at 2 o'clock, votes began on the floor, and as the gentleman knows, normally it is the procedure of this committee and all committees to permit members to discharge their obligations to vote on the floor of the House. It was the interruption in our schedule and this committee by votes on the floor that necessitated the postponement of the commencement of this hearing until the completion of those votes on the floor.

Second, the member from Massachusetts is an outstanding participant on this committee, and I understand the motivation behind his questions; it is one that I appreciate and share. Members of this committee who wish to participate, in my view, should be incentivized by our rules and by our practice; and as chairman of the full committee, that would certainly be my aim and my design.

And third, when the gentleman refers to the Chair, I think he recognizes that while I am the chairman of the full committee, I was not the chairman—this is a subcommittee meeting—I was not the chairman who convened this meeting. But it is my practice in the full committee, and I would urge all the subcommittee chairmen to make it their practice in the subcommittees, to interpret the rules in such fashion that members are accorded the utmost degree of fairness.

It is my practice in the full committee to use the list of minority members in the order of their appearance that is provided to me by the ranking member on the committee and by the minority staff. I don't get into the business of which minority member should be preferred over which other, because I think our rules can be implemented with punctilious fairness if they are administered by the majority and the minority in that way.

So that would be my guidance for all the members on the committee and, in particular, for members wielding the gavel on subcommittees. And I hope that is satisfactory to the gentleman.

I do want compliment the gentleman for his presence at these hearings. He is—I don't want to say anything about the members that aren't here, but for those members that are here, I want to thank you. I know other members—all members have pressing business, and your presence here is a testament to your commit-

ment to the subject matter, and I think a compliment to the witnesses.

Mr. MARKEY. I would like to reclaim my time just to make two points.

One is that the roll calls had just gone off. And in the Energy and Commerce Committee, on which I have served with you, in most instances, the Subcommittee Chair just continues the statements of Members until there is approximately 5 minutes left to go; and so, if the hearing has started at 10:00 or 2:00, then the Ranking Member and the Minority Member would then try to get their opening statements in, and then say, We will adjourn and then come back. And that would be the practice and tradition in other committees that I serve on, at least Natural Resources and Energy and Commerce.

On this Committee I was told not that there would be any flexibility whatsoever and not that punctilious fairness would be the rule here, but rather punctilious rigidity, and that rigidity was going to be imposed upon me; and the Majority Counsel informed me of that, even though it seemed to me that that was an implementation of the letter, but not the spirit of how a Committee should be governed.

And I just think that for the Minority, we have to have some sense of what will happen if this very same circumstance occurs. And saying that there should be punctilious fairness, yet not define what that means—and as you know, you are going to have to deal with that in your new position at the Securities and Exchange Commission—a fairness opinion that is issued by Goldman Sachs on a deal to which Goldman Sachs is a partner may not actually have fairness in it for investors; it may only have fairness to Goldman Sachs and for the other deal-makers.

So—fairness is also subject to interpretation, so I would wonder here, Mr. Chairman, what kind of tradition could be established in terms of what it means in terms of recognition for the minority.

Mr. COX. I would yield to the gentleman from Massachusetts for purposes of colloquy with the gentleman from Washington.

Mr. MARKEY. I would be glad to yield.

Mr. COX. The gentleman refers to the Committee on Energy and Commerce presumably as a useful model; the Gentleman knows that I am an alum of that Committee, and that was, in fact, the model for our rules in this Committee. To the extent we can have a very clear pattern and practice that doesn't take any Member by surprise, that is what we are aiming for here.

So, to reiterate, the rule is, as the Gentleman discovered, the Members present when a hearing commences and the gavel falls are recognized in order of seniority. Thereafter, Members are recognized in order of seniority—in order of appearance.

Mr. MARKEY. May I ask, Mr. Chairman? So, for example, if the Democrats arrive and it is 2 o'clock, but the Majority is still caucusing in the next room, and the majority does not emerge from their caucus until 2:20, even though the hearing was called for 2:00, are the Members here for the appointed time; or is it only at the point that the chairman brings down the gavel?

When does the Minority arrive? Is it strictly within the discretion of the Chair at that point in time, even though—the class has

started at 2:00; if the professor doesn't arrive until 2:20, weren't the students there on time? Or is it the hearing which is actually late, not the Members?

Mr. COX. There are two points that I was going to make. The first, I have already made, which is what the rule states.

The second is, the practice that I have followed as Chairman of the full Committee, that I would urge my Subcommittee Chairmen to follow, unless I hear an objection from Members, is, the order of appearance—your questions all go to that—and, thus, the order of recognition for Members should be determined on the Majority side by the Chairman, the person presiding over the hearing, and on the Minority side by the Ranking Member or the person who is Ranking at that time.

I don't see any reason for me, as Chairman, to determine in which order the Minority members should be recognized since we all understand what the rules are, and since it would eliminate any potential for unfairness if the ranking member gets to determine the order in which Democratic Members are recognized. That is the procedure I followed in the full committee; I have found it works very well, we haven't had any complaints of this type. I hope we don't have any unnecessary and certainly unintentional bumps in the road such as this.

But let me just return to the point that I made earlier, which is that I understand the Gentleman's interest in participating in these hearings, admire his willingness to be here when I observe others are not.

I would also observe that we have some witnesses on the second panel that are anxious to testify, and a witness on the first panel that you are entitled to question for 5 minutes, at such time as you wish to commence.

Mr. MARKEY. I am ready to begin.

Mr. COX. The Gentleman is recognized for 5 minutes.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. Stephan, up until now, the Bush White House has essentially given the chemical industry a terrorist take-home exam; that is, the chemical industry just gave itself its own grade, which obviously was a very dangerous situation for the Bush administration to leave our country in for the last 4 years in terms of these very dangerous chemical facilities.

My question to you would be, then, specifically, would the Bush Administration support legislation that created mandatory, enforceable, risk-based Federal standards for chemical facilities, with the highest priority being given to facilities that have the potential to harm the most people?

Mr. STEPHAN. We are—as I said in my oral testimony earlier, sir, we are seeking to cooperate with Congress in reaching a legislative solution that would provide the Secretary of Homeland Security certain authorities that the Secretary does not have in order to implement a risk-based, regulatory regime in a measured, calibrated manner—

Mr. MARKEY. And would you support that that legislation be mandatory and that the standards be enforceable?

Mr. STEPHAN. That the standards be measurable and enforceable.

Mr. MARKEY. And mandatory.

Do you want the Congress to provide mandatory—

Mr. STEPHAN. That is correct, on a risk-based model.

Mr. MARKEY. With the highest priority being given to those that have the most potential harm to the most people?

Mr. STEPHAN. That pose the greatest risk, taking into account threat, vulnerability and consequences.

Mr. MARKEY. As you know, in the nuclear area, the Nuclear Regulatory Commission allows Wackenhut, a security company that provides protection for the nuclear power plants in our country, to actually do the force-on-force test for the power plants that Wackenhut provides the security, which, of course, calls into question again the terrorist take-home-exam quality to that.

Would the administration support legislation that required the DHS to evaluate the chemical facility security using force-on-force exercises with entities that are independent of the security forces that are at these chemical facilities?

Mr. STEPHAN. Sir, for the record, I do not have the authority from my boss to go into any specific details, many of which are under development, in reference to specific authorities that would be requested to support the Secretary's approach to Congress.

Mr. MARKEY. So you are not willing to commit to having force-on-force tests of the chemical facilities across the country?

Mr. STEPHAN. Sir, I am not willing to commit or not commit to anything that involves a specific, prescribed regulatory—or aspect of this regulatory regime that is still under development at this point.

Mr. MARKEY. Do you believe that that makes sense, to do force-on-force tests of the security around chemical facilities?

Mr. STEPHAN. Sir, again, I am not going to be in a position at this point in time to go into any further details.

Mr. MARKEY. I will then tell you that I believe, that will be a huge, huge loophole in the security around chemical facilities if there are not independent force-on-force tests which are given to the chemical facilities. And the fact that the Department of Homeland Security, at this late juncture, 4 years after 9/11, still does not have a view on that indicates a very, very dangerous situation may continue to exist around chemical plants because without the test on security, force-on-force, and the fact that the Department right now has no view on it indicates that we could very well wind up with a situation that is still very dangerous.

Next question: Would the administration support legislation that required companies to reduce the risk their facilities posed by taking steps to reduce toxic chemicals or processes with less dangerous technologies when it is economically and technologically feasible for them to do so?

Mr. STEPHAN. Sir, in my earlier testimony, I stated that the Department supports a regulatory approach that involves a certain set of standards based on risk. There would be flexibility built into such a system to allow the companies the ability to draw upon various options in order to meet that standard. As long as the standard was met, we would like to keep the menu of options open to the companies.

Mr. MARKEY. So that would be a "no," you are not going to have a requirement that they have to convert to less dangerous materials?

Mr. STEPHAN. Sir, again, at this point in time, I am not authorized to get into any further level of detail with respect to the exact specifics of the regulatory regime we have proposed.

Mr. MARKEY. And again, I would say that if you do not do that, then we will continue to have an unnecessarily high level of dangerous toxic materials in urban areas, even though the Department of Homeland Security would have the ability to mandate that they do begin a conversion process over to less dangerous materials.

And finally, would the administration support having whistle-blower protections for anyone who is retaliated against for reporting chemical security flaws, so that we have at least as strong a standard as shareholders have in the financial services marketplace in terms of employees under Sarbanes-Oxley being able to blow the whistle on dangerous activities without being retaliated against?

Would this administration support whistle-blower protection for chemical industry employees while security—

Mr. COX. The gentleman's time has expired.

Mr. MARKEY. Who blows the whistle?

Mr. STEPHAN. Sir, at this point in time, I am not authorized to make any specific comments on any specific aspects of the regulatory regime that we would like to work together with Congress on over the coming weeks.

Mr. MARKEY. Again, Mr. Stephan, these are the key issues that you are going to have to deal with, and making an announcement that you are moving in this direction without providing the specific details will not offer real comfort to those who are concerned that Al-Qa'ida is targeting chemical facilities at the top of their list.

Thank you, Mr. Chairman.

Mr. COX. The Gentleman's 15 minutes have expired.

The Gentleman from New Mexico.

Mr. PEARCE. Thank you, Mr. Chairman.

I am wrestling, Mr. Stephan, with the concept of risk. It appears that we are thinking in terms of risk as some event and then in the surrounding population how it is affected; is that an adequate description of the threat level?

Mr. STEPHAN. No, sir. I would say that from Secretary Chertoff's perspective, risk is made up of three variables—consequences, vulnerabilities, and threat.

Mr. PEARCE. And if you are talking about consequences, could you give me some other description about how those consequences have been—how we have been describing them, how we have been talking about them in the discussions?

Mr. STEPHAN. Sir, consequences could mean public health and safety factors in terms of possible fatalities, possible injuries resulting from an exposure to a chemical agent in the context of this sector. It could be economic impact in terms of, does a chemical facility represent a risk because it is the only or unique producer of a certain component that is critical for some Department of Defense deployment capability, so on and so forth.

It could be, Where does this particular facility lie in the supply chain in terms of an impact against this facility, impacting distribution of the chemicals produced at that facility across the border? It refers to psychological dimensions in terms of how would the American public perceive and react to an attack upon this type of infrastructure target versus another, and so on and so forth.

Mr. PEARCE. Have we had discussions then about, for instance, if there is some sort of manipulation of the food chain—here are large cheese and milk plants in the district that I represent—and do those discussions give equal consideration to problems that might be not in large population areas, but entered into the food chain that are then distributed through a supply system throughout the country?

Are those recognized as significant threats in the same context that your discussion about the chemical plants have been recognized?

Mr. STEPHAN. Yes, sir. Generally the answer to your question is "yes," but I want to get back to the chemical piece.

As we do this risk assessment and methodology in partnership with our private sector owners and operators, we are building in, in terms of the consequences piece, estimates of how interconnected that particular facility—of the systems that are onboard the facility, what that means to the rest of the greater world around them within the chemical sector and across to other sectors.

Mr. PEARCE. How many chemical facilities, if successfully attacked, would have consequences on the scale of 9/11?

Mr. STEPHAN. Sir, I would have to get back to you with that kind of information. I don't have those statistics.

Mr. PEARCE. Is it a small number? In other words, you all have been wrestling with this concept—

Mr. STEPHAN. Sir, I don't want to get into an exact number that I will not be able to defend.

Mr. PEARCE. I am just trying to get from my own sense here, if we have a great number or if it is a small number. I am not trying to hold your feet to any fire.

Mr. STEPHAN. Using the EPA, again, the EPA Gross Potential Consequence Model, according to our estimations, the potential impacts—again, potential impacts between 50 to 500,000—we think there are about 260 facilities within that category. Again, that is based on the EPA, every single individual within a certain diameter circle around that facility.

Mr. PEARCE. The concern here about whether or not we can trust industry to have a disciplined approach to their own facilities, your testimony seems to indicate that Mr. Chertoff thinks that you don't have enough regulatory capability, but your testimony indicates that you may even have pretty good participation.

How close can we get to full compliance if we just have industry working with you on a voluntary basis or on the seat-at-the-table basis that you have been kind of exploring right now?

Mr. STEPHAN. Sir, I believe, again, there is about 20 percent of industry that would be important to us in terms of high risk that is not accounted for under the Responsible Care Code, or the MTSA regime. And within the Responsible Care Code, I think it is important that we have the ability into the future to measure the effec-

tiveness of the investments that are being made and the enhancements that are being implemented across the Responsible Care Code voluntary regime.

Mr. PEARCE. Thank you, sir.

Thank you, Mr. Chairman.

Mr. COX. The Gentleman from Washington is recognized for—

Mr. DICKS. Just one quick question.

How long is it going to take the administration to be able to come up with their legislative recommendation—week, 2 weeks, a month?

Mr. STEPHAN. Sir, within the coming weeks I am dedicating the most talented brainpower I have to figure out this regulatory structure and put it into the homeland security counsel process. So I don't have an end stage in mind, other than we are working aggressively now to come up with filling in the details of putting flesh on the bones of the skeleton.

Mr. DICKS. Well, the sooner, the better.

Mr. STEPHAN. We agree.

Mr. DICKS. Thank you.

Mr. COX. Does the Gentleman from New York seek recognition?

Mr. KING. Mr. Chairman, unfortunately, I missed the other part of the meeting; I have had other meetings. I would be glad to yield my time to any of the other gentlemen if they—

Mr. COX. Well, if the gentleman did seek recognition, I would ask unanimous consent that he be recognized, but if he does not wish to be recognized, we would move to the next panel.

Does any other member seek recognition to question Mr. Stephan?

If not, I want to thank you very much for your outstanding testimony, your help to this Committee today.

Mr. STEPHAN. Thank you, Mr. Chairman and Members.

Mr. COX. The witness is excused, and I call up our second panel for testimony.

The Chair would welcome the second panel comprising Mr. Frank Cilluffo, Director of Homeland Security Policy Institute at the George Washington University; Mr. Stephen Bandy, Manager of Corporate Safety and Security at Marathon Ashland Petroleum, testifying on behalf of the National Petrochemical and Refiners Association and the American Petroleum Institute; Mr. Marty Durbin, Managing Director of Security and Operations at the American Chemistry Council; Mr. Allen Summers, President and CEO of Asmark Inc., testifying on behalf of the Fertilizer Institute; and Mr. Sal DePasquale, Security Specialist at CH2M Hill and the Georgia State University.

Mr. COX. We will begin by recognizing Mr. Cilluffo, Director of the Homeland Security Policy Institute at the George Washington University, to testify.

STATEMENT OF FRANK CILLUFFO

Mr. CILLUFFO. Thank you, Mr. Chairman. And Mr. Chairman, distinguished members of the committee, it is a privilege to appear before you today.

I will be brief, not my strong suit, as I have barely had an unspoken thought, but I think we have had a long day.

I think I speak for everyone when I say we all have the common goal of best protecting the chemical industry and, obviously, our Nation's citizens from the consequences of an attack. Where we may differ is in our philosophical beliefs on how we can best accomplish this mission.

My specific focus will be on the significance of a public/private partnership for homeland security. Such a partnership is not an option, but rather a necessity, as the private sector, as we all know, owns a vast majority of the infrastructures that underpin our economy and will ultimately play the most important role in implementing any of those solutions. It is a shared responsibility where we must marry up private sector interests with public responsibility.

To this end, I contend we must build the business case for homeland security for the chemical industry, and beyond, to incorporate all the other critical infrastructures, because we can't look at this in isolation of some of the other infrastructures.

We want to reduce risks and mitigate the consequences of an attack on our chemical sector, and ensure that we are not merely shifting risks or creating new ones or unforeseen ones. We must prioritize, as I think the chairman and the members have all concluded, using a risk-management-based approach, and execute a strategy based on an equation of vulnerabilities, threats and consequences. Innovation, rather than the status quo, should be emphasized, since the terrorists are not static and base their actions on our actions—in fact, base their actions on many of our successes.

When faced with a public/private challenge, conventional wisdom is to search for an easy solution, regulations. But homeland security, I think, requires a more novel, nuanced approach if we are to actually succeed. Regulations often hamstring growth and innovation and lead to added expenses without taking industry's perspective into account.

Most importantly, they don't always provide a practical or a comprehensive solution. Regulations often create a check-the-box mentality, where industry does just enough to meet the requirements and are disinclined from taking or making more proactive homeland security investments.

We cannot just place requirements that make us feel good. Instead, we must ensure that what we do matters, and that it is outcomes based, very carefully calibrated, as I think Assistant Secretary Stephan referenced.

A successful business case for homeland security should include at least five key concepts, which I will now discuss: first, public/private coordination and information sharing.

The Federal Government has significant expertise and, of course, the intelligence information on the adversaries that the chemical sector will need to successfully implement its roles and responsibilities. The chemical sector obviously owns the infrastructure that the government is endeavoring to secure—and I might note, they are as well.

The government can provide the framework and industry, as experts in their field, develop standards. All information, from time-sensitive threat information to best practices should be part of a

trusted information-sharing effort that flows both ways, top to bottom, bottom up, and horizontally. A prime example of this I think is FedEx's participation on the FBI's Joint Terrorist Task Force, an unprecedented role for industry and maybe something the chemical sector can learn from.

The essential point is that each side should see that it has something to gain by contributing. What we absolutely cannot afford is a double sunken cost where the private sector takes the initiative to invest on its own in homeland security, only to have it superseded by regulations requiring yet another cost.

Second, we must develop standards in metrics. The government needs to raise the bar and keep it high, ensuring that the standards by which the industry are judged are as clear as possible. Standards should be initiated by the private sector and overseen either by the Federal Government and/or another trusted third party. We need experts driving security, not the trial lawyers.

The government should indemnify those organizations that meet the standard from actions above and beyond those identified. Hence, the government, in essence, assumes the of role of the insurer of last resort, as is the case for conventional warfare.

In developing its own Good Housekeeping Seal of Approval, the Federal Government would create an industry-wide objective that everything across the entire spectrum in life cycle, the chemical cycle, would endeavor to fulfill. As the adage goes, what gets measured gets done. Thus, we must have metrics and ensure that what we are measuring actually matters, and that it is paying security dividends.

Third, we have to identify the secondary benefits to security. Like the successful efforts to improve quality in the 1980s and safety in the 1990s, we must embed security as part of the corporations' daily operations. Security and profits are not mutually exclusive concepts. A dollar spent on homeland security could mean a dollar saved, providing a double bang for the counterterrorist buck—forgive the bad pun.

Fourth, we must establish incentives. I haven't heard a whole lot on incentives today, but I think on any CEO's wish list of outcomes from a proactive security strategy are lower insurance premiums, reduced legal liability, reduced tax liability, safe harbor provisions, recognition from the government and its private sector peers, enhanced reputation, and reduced incident response and recovery costs.

Mr. CILLUFFO. Beyond the government's responsibility to develop incentives, the private sector too has a role to play. The insurance industry in particular has tools at its disposal that could effectively induce good behavior. Just as the insurance industry drove to more stricter building codes and a focus on fire prevention rather than only responding to fires, so too could the insurance industry incentivize the chemical sector to take more proactive action. Few can argue with the results of the insurance industry's drive toward fire prevention. Countless lives saved and billions dollars of property damage averted was obviously a wise investment.

Fifth, we must recognize performance. The Federal Government should publicly commend corporations' accomplishments with an award akin to the Malcolm Baldridge Award, something that every-

one strives for which ultimately led to ISO 9000 standards and everyone sought to be recognized.

Finally, and much of the discussion today, I reluctantly add that we can enact regulations if necessary. And here, I say if and only if the market is unwilling or unable to meet the bar, those standards, increase DHS oversight and regulation should be carefully considered. And I think it needs to focus on the high risk facilities you identified earlier.

However, we must realize that regulating the chemical sector could quickly become a slippery slope for other critical infrastructures and sectors of the economy as well. Given the constantly evolving threat, we must not turn to a one size fits all approach and create regulations that could lose utility with the next Intelligence Estimate. It is always my contention that we should mitigate before litigate or regulate and I think a successful business case can help forestall most of those regulations.

In closing, the chemical industry is the focus of the hearing, but the strategies we discussed today can be translated to a dozen other critical infrastructure sectors. Spending alone, whether government or private dollars, will not thwart terrorist attacks to critical infrastructure. It takes the collective actions and the commitment of the government and the private sector to constantly refine our strategies to secure the facilities critical to our Nation. Above all, we cannot afford for our slow action to lead the public to lose trust in our ability to secure the Nation. That is at the heart of today's hearing.

Mr. Chairman, this concludes my statement and I would be happy to try to answer any questions you may have.

[The statement of Mr. Cillufo follows:]

PREPARED STATEMENT OF FRANK J. CILLUFFO

Chairman Cox, Chairman Lungren, Ranking Member Thompson, Ranking Member Sanchez, and distinguished members of the Committee, it is a privilege to appear before you today. The House Committee on Homeland Security should be commended for continually reassessing and reevaluating our efforts to secure the nation's critical infrastructure, including today's issue, the chemical industry.

Recognizing the important roles that the private sector and the government play, the Committee has assembled a cross-section of the chemical industry as well as the Department of Homeland Security. This is important because Congress must understand both perspectives to receive a complete picture of accomplishments, and areas for improvement, since 9/11. My specific focus will be on the significance of a public-private partnership for homeland security policy. To this end, I will delineate how we can establish the "business case for homeland security" across the chemical industry and beyond. Each witness will have his own insights and recommendations regarding the threat and potential solutions, but we must not take our eye off the ball and allow our individual interests to obstruct the overall mission.

We are all meeting today with the common purpose of better protecting citizens by ensuring that the nation is doing all it can to bolster security. But we have a few questions to answer. As a key component of the nation's critical infrastructure, what are this sector's roles and responsibilities? What are the federal government's responsibilities? What do we measure and are we measuring the right things? And, how much is enough? My hope is that the solutions discussed during today's hearing can serve as a foundation for future legislation and strategy as we continue to refine our tactics to fight the war on terrorism. We must also not limit ourselves by looking at the chemical industry in isolation—as many of the issues we face in this sector are relevant to protecting critical infrastructure writ large. Homeland security requires a multifaceted strategy to prevent, protect against and respond to 21st century threats. We need to develop further guidelines to help us build upon the significant progress we have made thus far in securing our nation's chemical sector, but we must consider all aspects of a solution—constantly developing new approaches

to the problem. We cannot rely solely on yesterday's weapons and strategies to fight tomorrow's battles and defeating a dynamic network of enemies will require our own dynamic network of domestic and international allies that will include all levels of government, the private sector, communities and individuals.

Terrorists turned commercial planes into missiles on 9/11, swiftly and viciously awakening the nation to the challenges before us today. It was eminently clear that the war on terrorism would not be anything like the wars of the previous century and the new enemy shares little in common with the previous one. Al-Qa'ida and its ilk do not exhibit traditional characteristics or fall under any conventional military definitions, representing an asymmetrical, constantly morphing threat that is symbolic of the challenges we now face. Terrorists targeted the symbols of the nation's public and private sectors on September 11, as they struck both the World Trade Center and Pentagon, negating the traditional, centuries-old security barrier of two large oceans. We now face an enemy consisting of a network of affiliated groups who span national borders and jurisdictions and use non-traditional weapons in battle without distinguishing between soldiers and civilians. We do not face an adversary that we can defeat in a conventional war on a traditional battlefield by going plane for plane or tank for tank, but one that will take the path of least resistance by constantly searching for our greatest vulnerabilities. They have declared war on every American and threaten all segments of the U.S. economy and with that, the global economy. Bin Laden has repeatedly said he intends to "[bleed] America to the point of bankruptcy."[1] Recognizing the enemy's strategy, we must embolden the industries that underpin our nation's economy. We now fight a war that requires us to play both offense and defense, pursuing the terrorists abroad and keeping them on the run, while also bolstering our defense at home. Experts agree that an attack on the nation's chemical sector, which includes more than 15,000 facilities engaged in the production, use, storage and distribution of toxic products, could have potentially catastrophic consequences.

Against this background, we must understand that this is not a war that can be solely fought and won in Washington but needs the innovation, hard work and input from individuals across all sectors of the economy. It is more than just guards, guns and gates. The thousands of private sector companies that own and operate the energy, banking, finance, agriculture, telecommunications and chemical sectors, among others, underpin the American economy, and all have a significant role to play in our strategy. Given the interdependency of all of the sectors, a unanimous commitment will be essential. The war on terrorism is the calling of our generation and we must adapt our existing organizations, structures and processes to meet the new threat. Innovation, rather than the status quo should be emphasized since the terrorists are not static and base their actions on our actions. And because of the constantly evolving threat, we must always strive to stay ahead of the curve. The bureaucratic structures and strategies of the past will not adequately meet the challenges of the future, and a new organizational paradigm is vital to confront emerging threats and enemies. We must marshal and mobilize all of the available expertise and latest technology in the private and public sectors as we devise and execute a comprehensive strategy to win the war. But we also cannot make the mistake of looking for new solutions through our rearview mirror. Rather, we need to view homeland security through a prism, considering every perspective and how each company, industry or department fits within the overall mission. We do not want to be in a position where we are constantly reacting to their actions—as the adversary adapts, finding our next greatest weakness. Thus it is necessary to address all potential threats in a proactive manner.

We want to reduce the risks and mitigate the consequences of an attack on our chemical sector and ensure that we are not merely shifting risks and creating new, unforeseen risks. We must prioritize, using a risk management-based approach that looks at homeland security holistically, and execute a strategy based on an equation of vulnerabilities, threats and consequences. The approach can be applied to all levels of government and the private sector as we define and redefine our priorities in the years to come.

Recognizing that the private sector owns and operates more than 85 percent of nation's critical infrastructure, a public-private partnership for chemical security is both sensible and necessary. The government's control over the production, use, transport and distribution of at-risk chemicals is limited and comprehensive security requires the concerted investment and support of the private sector. The *National Strategy for Homeland Security* notes that "a close partnership between the government and private sector is essential to ensuring that existing vulnerabilities to terrorism in our critical infrastructure are identified and eliminated as quickly

[1] Statement by Osama bin Laden, November 1, 2004.

as possible."[2] Further, the *National Strategy for Physical Protection of Critical Infrastructures and Key Assets,* calls for this to be a "shared responsibility."[3] I could not agree more with this sentiment and fervently believe we need to look at the entire supply chain as we refine our strategy.

The government has made tremendous strides since 9/11 in securing our critical infrastructure. Key players in the chemical industry have also made significant advances to upgrade security—meeting both business and national interests. What we now need is for government and industry to work together to develop a playbook that they can use to drive planning and preparedness. A comprehensive assessment of where the industry is in terms of security accomplishments needs to be completed as we draw a roadmap for the future. This cannot and should not be a one-size-fits-all approach, but instead should be catered to the unique strengths and weaknesses of each industry.

When addressing homeland security issues and the public-private relationship, conventional Washington wisdom is to search for an easy solution, often turning to regulation and mandating industry to comply with new federal requirements. But homeland security requires a more novel, nuanced approach if we are to succeed—one that will obligate the government to veer from the standard practice of pronouncing new "though shalts." Regulations often hamstring growth and innovation, and lead to added expenses without taking industries' costs, concerns and previous measures into account'simply, they do not provide a practical or comprehensive solution. We cannot just place requirements that make us feel good; instead we must ensure what we do matters. A December 2004 report on cybersecurity issued by this committee's Subcommittee on Cybersecurity, Science, and Research & Development, concluded that "it is important to realize that industry may be incentivized to do more than government could regulate."[4] I agree and contend that this conclusion is appropriate for the chemical industry as well. Regulations can create a "check the box" mentality, where industry does just enough to meet the requirements and are disinclined from making proactive homeland security investments.

We need the experts driving security, not the trial lawyers. I have found that industry is generally willing to participate in security initiatives and adopt the government's goals and mission if they are viewed as a partner in the policymaking process. It is up to government to engage the business community and articulate why such initiatives are mutually beneficial to both the public and private sectors. The government needs to set the bar and raise it high through leading by example and getting its own house in order. It can help drive best practices and standards that can then be overseen by DHS and/or a trusted third party. The private sector should be asked to take security as far as it can, but since industry will not always be able to reach the bar on its own, the government must work with the private sector to help it meet the goals it set. The government and the insurance industry can provide incentives/aid to industry to help meet those standards.

We all understand that security and safety are tightly interwoven in the post–9/11 world and we need to look at chemical industry security using an all-hazards approach. We do not need "satisficing," which only leads to an industry vying for the lowest common denominator. So as we build upon recent private and public sector initiatives, how can the government make a compelling business case for homeland security that satisfies all parties and most importantly, betters the security of our citizens?

The Business Case for Homeland Security

In an April 2005 speech to business leaders at the U.S. Chamber of Commerce, Secretary of Homeland Security Michael Chertoff appropriately stated:

"We want to defend our country, but we also want to defend our way of life. . .Our goal is to create a security environment that works with the grain of commerce and doesn't cut against it, and that takes advantage of and leverages with the great American ingenuity, which is our principal weapon."[5]

The government is eminently well-suited to lead in some areas while the private sector has its own unique strengths. What we must do is marry-up private sector interests with public responsibility. The solution will require a private-public partnership that looks at the entire supply chain and approaches security using a risk

---

[2] *National Strategy for Homeland Security.* The White House, July 16, 2002.

[3] *National Strategy for Physical Protection of Critical Infrastructures and Key Assets,* The White House, Feb. 14, 2003.

[4] *Cybersecurity for the Homeland,* Report of the Activities and Findings by the Chairman and Ranking Member. Subcommittee on Cybersecurity, Science, and Research & Development, Select Committee on Homeland Security, U.S. House of Representatives, December 2004.

[5] Transcript of address by Secretary of Homeland Security Michael Chertoff at the U.S. Chamber of Commerce, Washington D.C., April 29, 2005.

management model. We need to reduce risk while mitigating the consequences of an attack. A successful business case for homeland security should include the following:

- Public-private information sharing and delineation of roles
- Analysis and assessment of threats, risks and vulnerabilities
- Identification of the secondary, tertiary benefits of security
- Highlighting of best practices, standards
- Oversight by government and/or trusted third party
- Carefully designed metrics that ensure progress
- Rewards and incentives for security
- Regulations, as a last resort

Cultivating public-private coordination and information sharing—We must begin by fostering a trusted partnership between the federal government and the chemical industry based on cross-sector communication and information sharing. We need to refine the game plan based on a more symbiotic relationship which ensures significant and timely security progress. The federal government has significant expertise and the best information on the adversary (including intentions, capabilities and modus operandi) that the chemical industry will need to successfully implement its roles and responsibilities. And the chemical industry owns the infrastructure the government is endeavoring to secure. The government can provide the framework and the industry, as the experts in their field, develop voluntary standards. All information, whether time-sensitive threat information, best practices or vulnerability assessments, should be part of a trusted information sharing effort. The government must properly communicate the threat the industry faces, keeping the sector informed of the latest intelligence, realizing that this changes with time and is often difficult to predict.

Information should flow both ways, from top-down and bottom-up. At FedEx, for example, the company readily shares information with the government because the company's leaders feel they have a duty to protect the homeland. As FedEx CEO Fred Smith said to his peers in *Chief Executive* magazine: "By taking responsibility for shoring up points of vulnerability in the physical and Cyberspace worlds, companies can truly defeat those who would harm our way of business and our way of life. I urge all businesses to become partners with government in making our companies, our country and, ultimately, our world more secure."[6] Since action is stronger than words, I point to FedEx's participation on the FBI's Joint Terrorism Task Force (JTTF), the only such company in the nation to have such a role.

Those corporations that have developed best practices should then be encouraged to share these with the federal government as well as their colleagues in the industry. The government needs to ensure that the Freedom of Information Act (FOIA) exemptions and antitrust provisions passed in the 2002 Homeland Security Act remain and are strengthened to ensure continued information exchange. The development of the Homeland Security Information Network (HSIN), which serves as a real-time, two-way information clearinghouse for both DHS and industry is another important initiative. Other existing programs are in need of a reevaluation, however. One such program is the Protected Critical Infrastructure Information (PCII) Program, which lacks the protections, much less the incentives, that industry desires.

In promulgating Homeland Security Presidential Directive 7 (HSPD–7), President Bush clarified the need for cross-sector planning, information sharing, risk assessment and coordination. The president directed each federal department to engage its stakeholders as partners for the purpose of strengthening the security of our key industries. The Risk Analysis and Management for Critical Asset Protection (RAMCAP) initiative is a prime example of how cross-sector cooperation can make major headway in analyzing threats and vulnerabilities and sharing information. A cooperative DHS-chemical sector project begun late last year, RAMCAP will eventually lead to a more systematic analysis of terrorist threats on the nation's chemical sector and other infrastructure using a risk-based approach. Aspects of the project include the development of a Security Vulnerability Analysis (SVA) methodology that will provide each sector with the tools and metrics for the analysis of threats as well as supplementing the National Asset Database (NADB) with industry-specific information and screening tools. In short, it will help us define our greatest vulnerabilities, delineate the threat, and highlight best practices for the industry.

The chemical industry has a seat at the federal government's homeland security table with last June's formation of the Chemical Sector Council, overseen by 16 associations representing the spectrum of the chemical industry. Sector Coordinating

[6] Smith, Frederick W. "Securing American and the World." *Chief Executive,* December 1, 2004.

Councils are intended to bring together the critical infrastructure protection stakeholders from key industries together with federal, state and local agencies. The Chemical Sector Council identifies, prioritizes, and coordinates the protection of the chemical industry's infrastructure and facilitates information sharing for threats, vulnerabilities, incidents and best practices. Now that the industry groups are together, DHS should immediately develop a framework with these groups and identify mutually agreed upon incentives and timelines that would accomplish what all sides want: a better protected and prepared chemical industry. Such a partnership would provide a better investment of public and private dollars than regulations alone. The essential point is that each side should see that it has something to gain by contributing. The coordinating council also provides a mechanism for government-to-industry communication that will enable one to build upon the other's previous work and ensure that each side's roles and expectations are properly communicated. What we cannot afford is a "double sunken cost," where the private sector takes the initiative to invest on its own in homeland security, only to have it superseded by regulations requiring another cost.

Developing standards and metrics—As I previously noted, the government needs to raise the bar and keep it high, ensuring that the standards by which the industry are judged are as clear as possible. Standards should be initiated by the private sector and overseen by Uncle Sam and/or a trusted third party. Members of the American Chemistry Council (ACC) follow a self-initiated Responsible Care Management System, which requires companies to assess vulnerabilities and develop action plans, but the ACC includes less than 10 percent of at-risk facilities and the care code lacks fixed metrics and standards for quality control.[7] Industry-wide, definable standards are needed to ensure the more than 15,000 facilities currently regulated by the EPA are secure from terrorist attacks. Such standards and expectations must be clear for all actors across the supply chain from producers to transporters to distributors. For example, the government cannot reasonably expect the chemical industry to provide air defense for their facilities, a public good that few would argue is the responsibility of the private sector.

Standards must meet security requirements and ensure due care without bankrupting industry or the federal government. The government could then indemnify those organizations that meet the standard from all actions above and beyond their capabilities, hence the government assumes the role as the insurer of last resort, as is the case for conventional warfare. In developing its own "Good Housekeeping Seal of Approval," the federal government would create an industry-wide objective that every chemical production, transportation and distribution facility would endeavor to fulfill. It is not inconceivable that citizens, looking to invest in socially responsible companies meeting a government-approved standard, ask the federal government for a list of those organizations taking security seriously. Thus the standard could provide a financial benefit to industry, with the market, not the government driving security. Among similarly priced goods, the security seal of approval could be the difference among consumers.

We must have metrics to measure the needs of the chemical industry as well as its accomplishments. As the adage goes, "what gets measured, gets done." However, we must ensure that what we are measuring actually matters and that it is actually paying security dividends. There must be a time component in the metrics as well, given that there is an imperative for action almost four years after 9/11. What we are measuring and the actions taken as a result must be a balanced approach for a given industry, company, or geography, given the dynamic risk, threat, and vulnerability environments.

The standards developed should be overseen by the government and/or trusted third party. Currently, chemical plant security is primarily overseen by the EPA and DHS. The EPA regulates the 15,000 Risk Management Plan (RMP) facilities under the auspices of the Clean Air Act, but DHS now has lead responsibility for securing the nation's critical infrastructure. Protecting critical infrastructure is a security and emergency management priority and no longer strictly an environmental issue. We need to take a comprehensive view and defend against both intentional and accidental chemical incidents, requiring us to look at chemical plant security with the all-hazards approach to safety and security. Moving full authority for the development and oversight of standards of chemical facilities to DHS would provide the chemical industry with a single authority on security matters. Given the DHS

[7] "Homeland Security: Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed." GAO–05–631.T United States Government Accountability Office, April 27, 2005.

mission and the new reality, the department is particularly well positioned to provide leadership in this area.

Identifying the secondary benefits to security—Like the successful efforts to improve quality in the 1980s and safety in the 1990s we must embed security as part of businesses' missions by helping industry see the secondary benefits of security. Just as the Ford Motor Corporation adopted the mission that "Quality is job one" in the 1980s, in a post–9/11 world, security should be job one for the chemical industry. Industry discovered collateral benefits of quality assurance and safety, and it is incumbent upon the federal government to stress the manifold benefits of security for national interests and each organization's bottom line. The government must emphasize the importance of business continuity and that addressing security issues will help companies preserve market share and maintain operations during both manmade/terrorism-related and natural disturbances. Organizational resiliency and the effort to standardize processes across the entire supply chain will have long term benefits for business as they seek to cope with everything from terrorist attacks to supply shortages to worker strikes.

The role of Chief Security Officers and Chief Information Officers need to be strengthened within the organization. CSOs and CIOs should not be viewed as cost centers, but instead as integral components of the leadership team that position security as a benefit rather than an expense. This is an issue for the boardroom, not the backroom or the boiler room. Security and profits are not mutually exclusive concepts and there are clear economic benefits for investments in security. Investments in security are often considered against investing in other profitable parts of the organization. But it is clear that new revenue, new businesses, new products and other secondary benefits can be found through security spending. Companies can get a return on investment (ROI) in security and a number of companies are heeding the national call for homeland security'seeing the potential for security, as well as financial dividends. Asset visibility and tracking, standards development, collaboration within the supply chain and physical and personnel security can do a lot to secure the nation as well as improve organizational efficiency. For example, utilizing GPS systems and RFID tags to monitor chemical goods will enable industry to more predictably and accurately track the flow of products, find exceptions in the system and track security breaches—all economically significant improvements linked to improving security. Security upgrades such as digital video monitoring systems in chemical facilities can also assist in emergency incident management and theft reduction. The secondary benefits to background checks on personnel, reinforcing plant physical security and improving communication among supply chain parties all have obvious security and economic benefits and are avenues for the government and private sector to pursue mutual interests. A dollar spent on homeland security could mean a dollar saved—providing a double bang for the counter-terrorism buck. This concept is transferable to all infrastructure sectors.

Leaders in the chemical industry should be applauded for their self-initiated efforts to secure the homeland. Since 9/11, over $2 billion has been spent by ACC members alone.[8] The 140-plus ACC member companies operating more than 2,040 facilities have enacted laudable, self-imposed security standards. Representing 90 percent of the nation's chemical production, the ACC has moved the ball down the field, but we are still too close to our own goal line. Despite their significant spending, ACC members only represent 7 percent of the nation's at-risk chemical facilities, and pending assessments, it is unclear how much has been accomplished industry-wide.[9]

Companies outside of the chemical industry have made security a priority. At FedEx, more than 500 law enforcement officers now place terrorism at the top of their list of priorities—along with traditional needs like theft prevention. Implied here is that the company sees secondary and tertiary benefits of security, among them improved product control, tracking and overall efficiency. But individual attempts by the private sector can only go so far, just as government-initiated programs have limited utility. Coordination is crucial and a symbiotic relationship between the government and private sector is required to get us to the next level.

We need to develop and implement dual-use technology that shows the clear economic incentives of security. Recent government/shipping industry initiatives exemplify a viable business case for security. More than 9,000 importers and other shipping organizations have realized that they can increase efficiency, productivity and

[8] "ACC Enhances security at 2,040 chemical facilities; Supports security legislation." American Chemistry Council, April 26, 2005: *http://www.accnewsmedia.com/docs/2200/2131.pdf.*

[9] "Homeland Security: Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed." AO–05–631T. United States Government Accountability Office, April 27, 2005.

profits through security by engaging in the Customs–Trade Partnership Against Terrorism (C–TPAT) program.[10] The program requires companies to bolster security by protecting their supply chains from terrorists in exchange for quicker processing and fewer inspections. The government gets the security and assurances it is looking for and the private sector gets greater efficiency and revenue. The National Strategy for Homeland Security notes that benefits of security to industry are self evident, making the "internalization of. . .costs. . .not only a matter of sound corporate governance and good corporate citizenship but also an essential safeguard of economic assets for shareholders, employees, and the Nation."[11] To this end, the government needs to initiate policies that do more than stress the merits of "good corporate citizenship," and instead incentivize the chemical industry to secure the nation's hazardous chemicals by communicating the numerous benefits of security. Policy without resources is just rhetoric and the government needs to appeal to industry as good businessmen and good citizens. Society stands to benefit, not just in homeland security terms, but from the secondary environmental, health, safety and anti-crime benefits as well. The private sector could take much credit for these accomplishments, if the business case is adopted.

Establishing incentives—As I previously testified at a July 2001 hearing before the Joint Economic Committee, only "through leading by example can the government realistically hope for the private sector to commit the sort of effort—in time and resources—expected of them."[12] I stand by this statement and continue to advocate a paradigm where the government leads by example, getting its own house in order by setting standards and developing best practices. It can then provide incentives to the private sector to make security a priority, while avoiding regulation that could stifle the growth and the natural market flow. On any CEO's wish list of outcomes from a proactive security strategy are lower insurance premiums, reduced legal liability, reduced tax liability, safe-harbor provisions, recognition from the government and its private sector peers, enhanced reputation, and reduced incident response and recovery costs.

Some of these wishes can already be fulfilled through proper utilization of the SAFETY Act, a potentially powerful liability elimination tool for sellers and customers of anti-terror products and services. The SAFETY Act is particularly relevant for the chemical sector, as it provides an incentive to facility owners to invest in their own security. Facility owners purchasing SAFETY Act certified technologies or services increase their security (by simple virtue of purchasing security tools) and decrease their liability exposure. A facility owner knows that it is purchasing a valid, effective product thanks to the rigorous evaluation process the seller must undergo before any SAFETY Act award is granted by DHS. And, of course, the owner will also receive immunity from lawsuits. DHS can assist in encouraging the use of the SAFETY Act by granting its benefits to more technologies and services—and that is something Secretary Chertoff has repeatedly committed to doing.

We should consider having the federal government serve as the insurer of last resort, by assuming a burden above and beyond what the private sector and the insurance industry is able to bear. The government may also need to consider anti-trust exceptions that will encourage information sharing between competitors. These are not unreasonable and I believe can be accomplished if we build a solid business case for homeland security.

It is important to point out that it is not just about money, but also information. The previously cited December 2004 subcommittee report on cybersecurity also lists a number of the aforementioned incentives as ways the government can leverage the private sector in promoting security. These incentives equally applicable to the chemical sector, as they are to cybersecurity. And as the report states, legislative mandates cannot be "both a floor and a ceiling" since in a free market, regulation could lead to an unprofitable (and thus untenable) situation.

The private sector too has a responsibility to develop incentives. The insurance industry in particular has tools at its disposal that could effectively incentivize critical infrastructure owners and operators. Just as the insurance industry drove municipalities toward stricter building codes and a focus on fire prevention, rather than only responding to fires, so too could the insurance industry incentivize the chemical industry to take proactive action. The insurance industry already has a complex matrix of discounts to encourage good behavior of various kinds, from non-smoking to ergonomic shop floors. And though developing insurance models for terrorism is dif-

---

[10] Remarks by Robert C. Bonner, Supply Chain Security in a New Business Environment, Miami, Florida, April 21, 2005.

[11] *National Strategy for Homeland Security.* The White House, July 16, 2002.

[12] "Wired World: Cyber Security and the U.S. Economy." Testimony by Frank J. Cilluffo before the Joint Economic Committee of the U.S. Congress, June 21, 2001.

ficult (and some would say, impossible), it is possible to recognize that some proactive actions not only reduce losses from a terrorist attack, but also provide important safety and anti-crime benefits as well. This expected reduction in insurance claims should be passed along to the private sector in the form of lower premiums, which will in turn encourage other companies to take proactive, dual-benefit security measures.

Recognizing performance—For those corporations that meet the industry-set standards, the federal government should publicly commend the corporations' accomplishments, provide government incentives and encourage private sector incentives. The DHS Homeland Security Advisory Council and the Council on Competitiveness should be commended for their calls for a homeland security award for private industry akin to the prestigious Malcolm Baldrige National Quality Award. A parallel effort should be fostered by the private sector. For the chemical industry, a major national organization would seem to be well positioned to recognize the accomplishments of its own.

Enact regulations, if necessary—If, and only if, the market is unwilling or unable to meet the bar, increased DHS oversight and regulations should be carefully considered. However, we must realize that regulating the chemical industry could quickly become a slippery slope for other sectors as well. This could lead to a situation where, for example, the information and telecommunications sector becomes regulated as a knee jerk reaction. Given the constantly evolving threat, we must not turn to a one-size-fits-all approach and create regulations that could lose utility with the next intelligence estimate.

If regulations are enacted, the costs, both to the government as well as the chemical industry, must be considered. The costs for implementing regulations will be significant to both parties. For example, legislation proposed in the last Congress that would have provided DHS with regulatory oversight of the chemical industry was estimated to cost the federal government more than $200 million over the first five years.[13] And the chemical industry must understand that regulations do not necessarily mean that the government will assume all costs. Thus it is always my contention that we should mitigate before regulate or litigate and a successful business case can and should forestall most federal regulations.

Conclusion

The chemical industry is the focus of this hearing, but the strategies we discuss today can be translated to the dozen other critical infrastructure sectors. Security is not merely a challenge, it is an opportunity for us to put our heads together and surpass our own assumptions. The task is enormous, and it requires efforts on every front. We must learn from our successes, as well as our mistakes and refine our efforts accordingly. We cannot shy from this task because of its magnitude. We can and must overcome it. Spending alone, whether private or government dollars, will not thwart terrorist attacks to critical infrastructure. It takes the collective actions and commitment of the government and the private sector to secure the facilities that we all can agree are critical to our nation. Above all, we cannot afford for our slow action to lead the public to lose trust in our ability to secure the nation. That's at the heart of today's hearing.

As I conclude, I would like to congratulate Chairman Cox on his recent nomination to head the Securities and Exchange Commission. Your leadership on homeland security issues and commitment to making this committee a permanent, standing body (no easy feat) is widely respected and appreciated. The SEC will be in good hands upon your confirmation. And I will add that you will be in a unique position to look at the business case for homeland security in your new capacity. Chairman Lungren, Ranking Member Sanchez, Ranking Member Thompson, your leadership and vision on the issues is also to be applauded, and I look forward to continuing to work with all of you and your colleagues on this issue and other matters that arise in the future. Mr. Chairman this concludes my statement. I would be happy to answer any questions you may have.

Mr. COX. I thank you for your testimony. The Chair now recognizes Stephen Bandy, Manager of Corporate Safety and Security for Marathon Ashland Petroleum, testifying on behalf of the National Petrochemical and Refiners Association and the American Petroleum Institute. And may I say, Mr. Bandy, and to the rest of

[13] Congressional Budget Office, Cost Estimate for S.944, *the Chemical Facilities Security Act of 2003,* May 10, 2004.

our witnesses, the members of this committee first are enormously grateful for your being here.

Second, I apologize in advance. We had a discussion about the interruption of this subcommittee's business by floor votes. We expect there will be floor votes coming up sometime soon. And the entire House of Representatives has a date with the President at the White House at 6:00. That means when we do go to the floor we will probably be unable to resume the hearing. I am hopeful we will put all of your testimony on the record before we go to the floor to vote. Feel free since we have your written testimony to give us what you really think we need to get because this may be your only shot.

Mr. DICKS. We have to keep it at about 5 minutes per witness in order to do that.

Mr. COX. Mr. Bandy, thank you.

STATEMENT OF STEPHEN BANDY, MANAGER, CORPORATE SAFETY AND SECURITY, MARATHON ASHLAND PETROLEUM LLC

Mr. BANDY. Thank you and good afternoon, Mr. Chairman, Ranking Member Sanchez, and Members of the Committee. I want to thank the Committee for holding this important hearing today and 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 infrastructure.

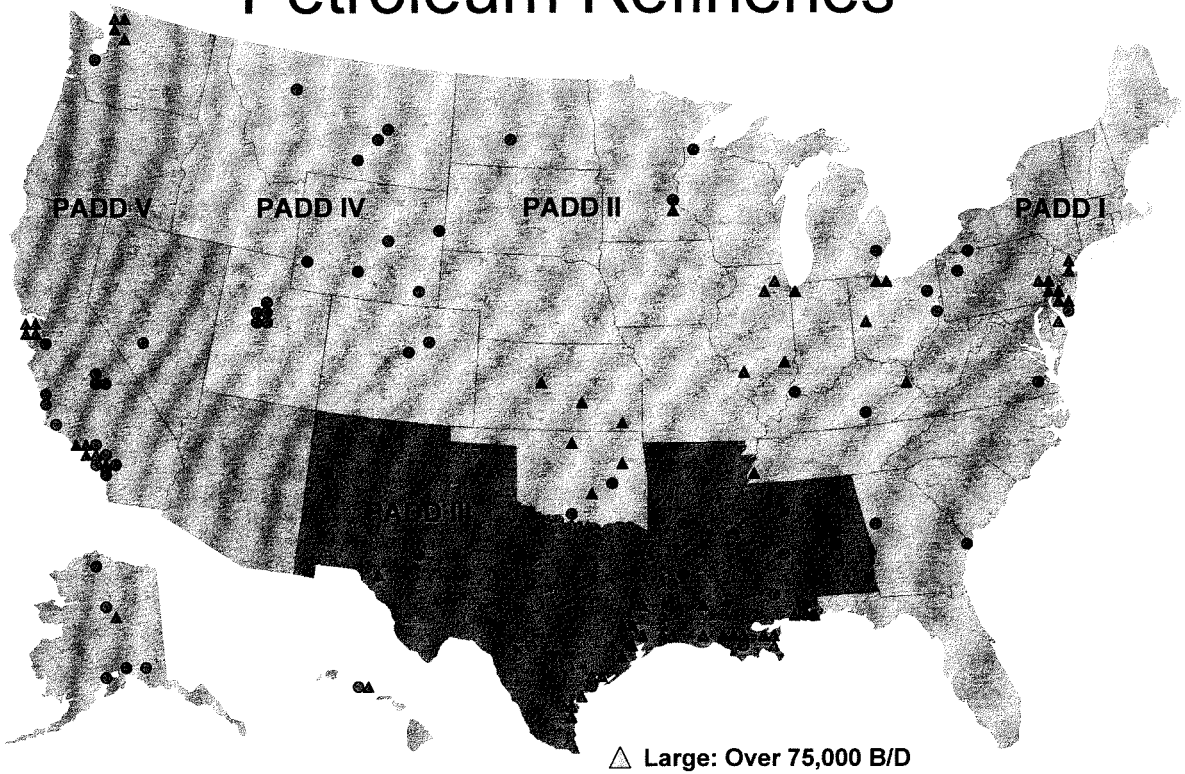
Maintaining the security of our facilities has always been a priority at refining and petrochemical plants. Our industry is heavily engaged and was so before 9/11 in maintaining and enhancing security. The industry has long operated globally, often in unstable regions overseas where security is an integral part of providing for the world's energy and petrochemical needs.

After the tragic events of 9/11, the industry, and I say this with special emphasis, did not wait for government regulations before implementing additional and far reaching facility securities measures to address these new threats. NPRA and API developed and provided industry with a peer review security vulnerability assessment methodology and DHS has endorsed this methodology and uses it to train its own employees. Our industry has employed the methodology to identify security hazards, threats and vulnerabilities, and evaluate and implement the best security measures possible.

In addition to the methodology, API developed security guidelines for the petroleum industry. The State of New Jersey has recognized these States as the States accepted petroleum industry practices. I would like to provide copies of these to the committee for the record, please.

[The information follows:]

Petroleum Refineries



EIA and NPRA

Mr. BANDY. Industry has also developed a close working relationship with over a dozen key Federal agencies as well as State and local law enforcement and to exchange real-time intelligence data on security issues that allows them to respond to threats. We have held joint training exercises, simulating actual terrorist attacks in developing educational programs with governmental agencies and sharing best practices to enhance security operations.

Media reports sometimes leave the impression that industry has not taken any new security initiatives since September 11. That simply is not true. With the critical information gained from conducting security vulnerability assessments, facilities have taken such steps as reconfiguring sites, allowing critical assets to be set back from the perimeter, install sophisticated state of the art electronic intrusion detection systems, implemented card access control with new biometric technology readers, required enhanced security communication systems, and shared security response plans with local law enforcement and appropriate Federal agencies.

The majority of the almost 150 refineries and 200 petrochemical manufacturing facilities in the United States are regulated by the Coast Guard under the Maritime Transportation Security Act. MTSA requires these facilities to conduct vulnerability assessments and submit comprehensive security plans to the Coast Guard. Our relationship with DHS and other agencies has been very effective in allowing industry to focus on the security threats that exist today.

To conclude, Mr. Chairman, our industry takes very seriously its responsibilities for strengthening securities. We will continue to work with DHS to maintain and improve the security of the refining and petrochemical facilities.

Thank you, and I will be happy to answer any questions.

[The statement of Mr. Bandy follows:]

PREPARED STATEMENT OF STEVEN P. BANDY

Introduction

Good morning, Mr. Chairman, Ranking Member Sanchez, 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 am the Manager of Corporate Safety & Security for Marathon Ashland Petroleum LLC (MAP), headquartered in Findlay, Ohio. As Manager of Corporate Security for MAP, I am responsible for ensuring the secure operations of our facilities for our employees, customers and the communities in which we operate. MAP is a refining, marketing and transportation company, with a complementary network of operations stretching across 21 states. We own and operate seven refineries and have a total crude oil capacity of approximately 948,000 barrels per day.

Today I am testifying on behalf of NPRA, the National Petrochemical & Refiners Association and API, the American Petroleum Institute. NPRA has more than 450 member companies, including virtually all U.S. refiners and petrochemical manufacturers, their suppliers and vendors. Petrochemical companies use 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 to medicine to computers. API, a 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.

Overview/Summary of Statement

Maintaining the security of our workforce, plant, property, and equipment has always been a priority at refineries and petrochemical plants. Refiners and petrochemical manufacturers are heavily engaged—and were so even before September 11—in maintaining and enhancing security. 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. NPRA and API member companies continue to address and prepare for potential threats to our facilities. We are absolutely committed to keeping all sites as secure as possible from threats of violence or terrorism. We are keenly aware of the responsibility we have to our employees, to our customers, and to the communities in which we operate. We have been working diligently to strengthen the security of our facilities, and in my testimony today I will outline some of the actions we have taken.

When the tragic events of September 11, 2001, occurred, we as a nation realized immediately that a vastly different set of threats had to be taken into consideration in order to protect our homeland. The refining and petrochemical industries were no different. 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. Industry consulted with and obtained the input of federal, state, and local agencies, first responders and other security experts who are knowledgeable about the strategy, tactics and plans employed by terrorists. That information, coupled with the knowledge that each company has about the specifics of its own technology and materials, was then used to conduct intensive security vulnerability assessments. Based on those assessments, detailed facility security plans were prepared and implemented.

Refiners and petrochemical manufacturers have taken and will continue to take additional measures to ensure facility security. We have developed close, working relationships with key federal agencies and state and local law enforcement offices to exchange critical infrastructure information. We have held joint training exercises simulating actual terrorist attacks and have developed educational programs featuring federal and state government officials with security expertise. We have sponsored association meetings to share best industry practices. This affords companies the opportunity to learn what others are doing, discuss new approaches and ideas, and implement the approaches that best fit their own particular security needs.

With those considerations as background, NPRA and API urge the Committee to consider the following comments regarding the current state of security-related activities at refining and petrochemical facilities:

- 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.
- Industry complies with security requirements under post 9–11 federal security law, such as the Maritime Transportation Security Act and the Patriot Act.
- A strong working relationship has been established between government security agencies and the refining and petrochemical industry to exchange "real-time" intelligence data on security issues that allows them to respond rapidly to terrorist threats.
- Industry has partnered with the Department of Homeland Security 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. (These will be discussed in more detail in my statement.)
- Industry supports full compliance with existing security regulations, adequate funding for DHS and other security agencies, and continuing public-private partnership efforts to protect facilities and vessels and strengthen intelligence-sharing networks.
- Congress has been wise to restrict public release of facility specific security information, the release of which would be disruptive to ongoing security operations.

Industry has conducted facility security vulnerability assessments.

In 2003, NPRA and API, working with other industry groups, the Department of Homeland Security and the Department of Energy, developed and provided industry with a peer-reviewed security vulnerability assessment (SVA) methodology. In 2004, industry expanded the SVA 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 operations for 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:

- Characterizing the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
- Identifying and characterizing threats against those facilities and evaluating them in terms of their attractiveness as targets for various adversaries, along with the consequences if these assets are damaged or stolen;
- 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 of an event 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.

Companies comply with security requirements under the Maritime Transportation Security Act of 2002.

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 the Maritime Transportation Security Act (MTSA) of 2002. (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 were reviewed and approved by the Coast Guard in 2004. Under the Maritime Transportation Security Act, companies are also required to designate facility security officers to 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 any 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.

I emphasize that 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 taken as a result of a dynamic process.

Industry sponsors educational programs and holds training exercises with government officials to enhance security at facilities.

NPRA and API have established standing committees on security; I am a past Chairman of the NPRA Security Committee and play an active role in the API Security Committee. NPRA has held or co-sponsored more than a dozen facility security conferences and workshops, featuring federal and state policymakers, security and counterterrorism experts, and the sharing of best practices. In February of this year, for example, NPRA conducted an intensive training workshop for persons designated as Facility Security Officers under the Maritime Transportation Security Act. The workshop enabled them to better fulfill their responsibilities under MTSA. Since 2002, API has been hosting training sessions for industry and government personnel to teach them how to use the vulnerability assessment methodology and develop security plans.

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 postulated 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.

In addition to the SVA Methodology, API developed the first edition of "Security Guidelines for the Petroleum Industry" in March 2002. It has since been revised and the third edition was released in April 2005. These Guidelines provide general guidance for effectively managing security risks and provide a reference to federal security laws and regulations impacting petroleum operations. I would like to provide a copy of both guidance documents, the SVA methodology, "API/NPRA Security Vulnerability Assessment Methodology for the Refining and Petrochemical Industries" and the "Security Guidelines" to the Committee and request that they be included as part of the hearing record.

Industry works with federal, state and local officials to enhance facility security.

The success of security programs in the refining and petrochemical industries is due in large part to the excellent working relationships our industry has established with various federal, state, and local governmental agencies. NPRA, API and their 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 receive updates on the latest intelligence about terrorist focus and targets. The agencies that 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.

Our relationship with DHS and other security agencies allows immediate access by government and industry to rapidly changing information affecting facility security. These relationships and communications are essential in keeping our facilities secure. If an agency is turned into an industry regulator through enactment of federal security legislation, the dynamics of the relationship will undoubtedly change and this level of information sharing could be diminished.

The American Petroleum Institute has worked with our state petroleum councils to disseminate the API Security Guidelines to assist their state agencies in preparing plans to upgrade security at our facilities across the nation. As an example, in New Jersey where the industry has considerable presence with six refineries and many terminals, former Governor McGreevey accepted the API Security Guidance as the state's accepted petroleum industry practices in October of 2003. Since then, the New Jersey Petroleum Council supplemented by company experts has been involved in educating state and local officials in security issues through regular meeting and training seminars.

Industry is working with DHS to improve risk assessment and to develop buffer zone protection plans.

Our 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 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.

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 with 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, and so our NPRA and API 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 and API members have also responded positively to a request to serve on a working group of the President's National Infrastructure Advisory Council.

One particularly important initiative underway—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.

Chemical security legislation would be counter-productive.

To conclude, Mr. Chairman, refiners and petrochemical manufacturers take very seriously their responsibilities for not just maintaining, but strengthening security at their facilities to meet any new threats. Our industry has complied with modernized, post 9–11 federal security requirements. We have utilized expert engineers who understand our facilities better than any one 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 business to capture the best practices to protect our facilities. And perhaps most importantly the industry has created an outstanding working relationship with government security agencies to rapidly receive the fast moving information needed to fight terrorism. This working partnership has been very effective in exchanging information to allow the industry to focus on the security threats that exist today and are most relevant. We look forward to continuing this security partnership. Our efforts show that industry does not need to be prodded by government mandates to take aggressive and effective steps to secure its facilities. In fact, industry is concerned that changing the nature of the existing relationship between DHS, other security agencies and industry could disrupt the open exchange and rapid response to threats that we have achieved to date. As a result, we are not advocating chemical security legislation because the existing system is working well, and, being a dynamic process, will continue to improve with time ..

In closing, I want to stress once again that NPRA and API member companies are absolutely committed to the security of our facilities. Thank you and I will be happy to answer any questions you may have.

Mr. PEARCE. Thank you, Mr. Bandy, for your testimony. The Chair now recognizes Mr. Marty Durbin, the Managing Director of Security and Operations for the American Chemistry Council.

STATEMENT OF MARTY DURBIN

Mr. DURBIN. Thank you, Mr. Chairman and members of the committee. I want to thank you for the opportunity to provide testimony today on behalf of the American Chemistry Council. ACC represent the leading companies in the U.S. chemical manufacturing sector responsible for nearly 90 percent of basic industrial chemical production and an essential part of our Nation's critical infrastructure. In my brief remarks, which I will try to make even briefer, I would like to highlight the following.

The leadership role that ACC members have taken to further ensure the safety and security of their products, their facilities, their supply chain and the communities in which they operate and investment of more than $2 billion in security since 9/11, 2001. I also would like to touch on the great strides made cooperatively by the Federal Government and our industry to secure the chemical sector, and finally what we see is a real need for Federal legislation to provide nationwide assurances that all portions of the industry take the same aggressive action that ACC members have taken.

Security is not new to our members but the tragedy of September 11 brought swift and decisive action from the industry leaders of our association. Without waiting for government direction, ACC issued site and transportation security guidelines in October and November of that year after which our board launched an aggressive effort to develop a new Responsible Care Security Code. Implementation of Responsible Care, ACC's signature program of continuous improvement in environmental, health, safety and now security performance is mandatory for all members.

The security code and ACC members' security enhancements have been widely and uniformly acknowledged by government as well as the media. State and local governments have used the code as a model for their own regulation of chemical facilities' security, and the Coast Guard, which as you heard regulates nearly 240 chemical facilities under MTSA, recognized our code as an alternative security program for ACC members.

Briefly, the code requires each member to prioritize every facility by risk, assess the vulnerabilities using methodologies developed by expert third parties, implement security enhancements commensurate with those risks, and to verify the implementation of physical security enhancements using outside third parties. All 2,040 ACC member company facilities have completed their vulnerability assessments, implemented security enhancements and nearly all have had their enhancements verified.

ACC security code also covers transportation and cyber security, allowing members to extend the reach of the code throughout the value chain. All the guidance materials developed by ACC addressing site, transportation and cyber security as well as the security code itself are publicly available through our Web site so they can have the broadest possible influence beyond our membership.

HSPD–7 specifically names DHS as the lead or sector specific agency for the chemical sector and we certainly think that is appropriate, and to achieve the infrastructure protection objectives of that directive ACC and its members and indeed the entire sector have worked in close partnership with the Department of Homeland Security.

Over the past years, everything from facility visits to working on the Buffer Zone Protection Plan, ACC funds and maintains the Information Sharing and Analysis Center, which is a public service of ACC through our program, and we participate regularly in exercises and drills, everything from local level preparedness and response drills to the national level TOPOFF exercises that recently concluded.

So why is Federal legislation necessary? Despite all the progress that has been made to date, there is no way to assure all chemical

facilities that need to be protected are taking the same kinds of aggressive steps that American Chemistry Council members and others have taken to protect this critical sector. ACC has led the effort to ensure all chemical facilities are secured. We have worked continuously with Congress and the administration for enactment of national security legislation that will establish national standards for security at chemical facilities, require facilities to conduct vulnerability assessments and implement security plans and provide oversight, inspection and enforcement authority to the Department of Homeland Security.

Without Federal action on this vital topic, State legislatures will fill the void. Both Maryland and New York have enacted chemical facility security laws. While ACC was able to support both of these statutes, we strongly believe that a national program, not an incomplete patchwork of potentially conflicting State efforts is necessary.

Naturally, we believe any Federal legislation should respect ACC members' substantial actions and investments to implement the Responsible Care Security Code. As witnesses at an April Senate hearing concurred, ACC members deserve a level playing field and a common set of expectations. But let me be clear, we are not asking for an exemption from the law, only that DHS be allowed to recognize our members' significant actions such as the Coast Guard has already done.

In closing, I want to reiterate our commitments. Our member companies are committed to taking all reasonable actions to enhance the security of their operations and products against those that would do us harm, but our Nation will not be safe until all chemical facilities that need to be protected have taken steps equivalent to those taken by our members.

It has been over 3–1/2 years since 9/11. Now is the time to act and we welcome this hearing. We are committed to continuing work with this committee and others to see that legislation is enacted in this session of Congress. Thank you, and I would be happy to answer any questions.

[The statement of Mr. Durbin follows:]

PREPARED STATEMENT OF MARTIN J. DURBIN

Chairman Lungren and Members of the Subcommittee, my name is Marty Durbin, and I am the Managing Director for Security & Operations for the American Chemistry Council (ACC). I thank you for this opportunity to speak today on behalf of the Council's members on the important subject of security in the business of chemistry, a critical sector of America's infrastructure.

The 132 members of the ACC manufacture essential life-saving products critical to homeland security and life-enhancing everyday items that keep the economy moving. Our products are critical to daily life and crucial to efforts to combat the war on terrorism. We are essential to making Kevlar vests, night vision goggles and stealth aircraft. The products we manufacture are essential to the things that make modern life possible, from plastics to pharmaceuticals, from cars to clothing. And the products of chemistry are critical in many aspects of American life, including keeping our drinking water safe, supporting agriculture, and spurring medical innovations to prevent and treat disease.

ACC represents the leading companies in the U.S. chemical manufacturing sector, an industry which is the largest exporting sector in the economy ($91 billion), and employs one million people in America alone, with $460 billion in sales. Our members are responsible for nearly 90% of basic industrial chemical production. In addition, the U.S. chemical industry has the largest share of knowledge workers of any

industry, and it is the largest private industry investor in research and development.

Mr. Chairman, I welcome the opportunity to highlight four things for you and the subcommittee:

1. The leadership role ACC members have taken—at a cost of over $2 billion since 9/11—to further ensure the safety and security of their products, their facilities, their supply chain and the communities in which they operate;
2. The great strides the federal government has taken, in cooperation with the chemical sector, to secure the industry;
3. The need for national legislation to provide an appropriate federal regulatory role in chemical facility security; and
4. Our views on the important and frequently misunderstood subject of inherent safety.

I. ACC Has Taken a Leadership Role in Enhancing Chemical Security

Even before September 11, 2001, Council members had begun to address the challenge of terrorist threats to our operations, by developing site security guidelines for chemical companies. Our Board of Directors was actually meeting that sad day, and their reaction to those events was swift and decisive. We quickly completed and issued our security guidelines, and a companion set of transportation security guidelines, in October and November of that year.

In those uncertain months, we shared those guidelines with state and federal agencies, and we and OSHA posted them on our public websites to make them as broadly available as possible. We also partnered with EPA to hold regional security briefings for our members and other chemical companies, state and local government officials, and first responders.

In January 2002, our Board launched an aggressive effort to develop a new Responsible Care® Security Code. Now in its 17th year, Responsible Care® is ACC's signature program of ethical principles and management systems designed to continuously improve our members' safety, health and environmental performance—and now, their security performance as well. Implementation of Responsible Care® is mandatory for all members of the American Chemistry Council, as well as Responsible Care Partner companies, who represent chemical carriers, warehouses, logistics planners and others along the supply/value chain. In developing the Security Code, we consulted closely with plant-level Community Advisory Panels, and with first responders and government agencies at all levels. In June 2002, the Board adopted the Security Code.

The Security Code, and ACC members' security enhancements, has been widely and uniformly acknowledged, from the *Washington Post* editorial page [1] to Government Accountability Office reports.[2] Former Homeland Security Secretary Ridge has referred to it as a "model program." The State of New Jersey has recognized the Code as a "best practice" for chemical facility security. In addition, the City of Baltimore adopted a security ordinance that recognizes the Code as an alternative means of compliance, and Maryland legislation mirrors the Code. At a hearing held April 27, 2005 by the Senate Homeland Security & Governmental Affairs Committee, Chairman Collins declared that companies like ACC's members "should be commended" for the steps they have taken to date voluntarily to secure their facilities. GAO official John Stephenson focused particularly on the substantial work that ACC members have done implementing the Responsible Care® Security Code, stating that "ACC is very good."

The Security Code requires member companies to:

- Prioritize their sites by degree of risk, sorting them into four tiers. This process was begun before the Code was adopted, and every ACC member company completed it on schedule in June 2002.

---

[1] "Some of the biggest security gains have been made cheaply, sometimes thanks to unobtrusive, even private-sector initiatives. The 140 large companies that form the American Chemistry Council, for example—a group with both financial and practical interests in not having their chemical plants blown up—have created their own security code, internal communications system and inspectorate." THE WASHINGTON POST, p. A26 (May 27, 2005).

[2] "To its credit, the chemical industry, led by its industry associations, has undertaken a number of voluntary initiatives to increase security at facilities. For example, the ACC, whose members own or operate 1,000, or about 7 percent, of the facilities [handling large quantities of hazardous materials in the country] requires its members to conduct vulnerability assessments and implement security improvements." GAO, "Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown" (GAO–03–439, March 2003) at "Highlights."

- Thoroughly assess vulnerabilities, using rigorous methodologies developed by Sandia National Labs and the Center for Chemical Process Safety (CCPS), a program of the American Institute of Chemical Engineers (AIChE).
- Implement security enhancements commensurate with risks, and taking into account inherently safer approaches, engineering and administrative controls, and other security, prevention and mitigation measures.
- Verify the implementation of these physical security measures, using third parties that are credible with the local community, such as first responders or law enforcement officials.

All 2,040 ACC member company facilities have completed their vulnerability assessments, and almost all have completed their enhancement verifications. Progress in implementing the Code was verified by GAO in its most recent report on chemical facility security.[3]

Our Security Code is not just limited to physical plant security. It covers the complete "value chain" for chemicals, from suppliers to customers, including transportation. Value chain management is an area where we have a long and successful history of partnering with and supporting federal agencies to prevent the diversion of legitimate and essential chemicals that have the potential to be misused to make illegal drugs or chemical weapons. In fall 2002, the Council issued a detailed value chain guidance document to enhance the security of our products outside the fence line. Our members who also belong to the Chlorine Institute have, together with the Association of American Railroads, implemented a chlorine rail car security plan.

The Security Code also covers cyber security, to protect our highly computerized operations from being attacked electronically. Our members lead a broad Chemical Sector Cybersecurity Information–Sharing Forum to promote cybersecurity in our industry. In spring 2003 the Forum issued a cybersecurity guidance document. The Forum also launched a broad cybersecurity practices, standards and technology initiative through CIDX, the Chemical Industry Data Exchange. All of these guidance materials, and the Security Code, are available through our websites (*www.americanchemistry.com* and *www.rctoolkit.com*) so that they can have the broadest possible effect beyond our membership. The CIDX materials are similarly available at *www.cidx.org/CyberSecurity/default.asp.*

II. The Federal Government, Working with ACC, Has Greatly Enhanced the Security of the Chemical Sector

ACC and its members have worked closely with the Department of Homeland Security during its first two years of existence. We concurred with GAO's recommendations in 2003 that the federal government should develop "a comprehensive national chemical security strategy that is both practical and cost effective," and that should:

- "Identify high-risk facilities based on factors including the level of threat and collect information on industry security preparedness;
- Specify the roles and responsibilities of each federal agency partnering with the chemical industry;
- Develop appropriate information sharing mechanisms; and
- Develop a legislative proposal, in consultation with industry and other appropriate groups, to require these chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action."[4]

A. *Identify High Risk Facilities*

Starting in March 2003, DHS partnered with ACC to facilitate visits to our members' facilities. ACC also worked with DHS to develop methods for evaluating facilities based on potential physical and economic consequences. And even before the creation of DHS, the Coast Guard and state offices of homeland security or counterterrorism visited facilities to offer advice on enhancing facility security.

Today, DHS' Protective Security Division (PSD) and the Coast Guard are actively visiting chemical facilities, reviewing vulnerability assessments and security plans, understanding common vulnerabilities and developing plans, in conjunction with local law enforcement and responders, to protect facilities and their communities. Information gained from these visits supports the development of DHS's "Buffer

[3] Based on work conducted between October 2004 and March 2005, GAO stated: "All 10 of the chemical facilities we visited reported making significant progress in fulfilling the requirements of the security code." GAO, "Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges" (GAO–05–327, March 2005), at 5, 37. ACC members' implementation of the Code is discussed in detail at pages 17–21.

[4] See "Homeland Security" *supra* note 2, at 27.

Zone Protection Program" to provide support and resources to local governments in plant communities. ACC is also working closely with PSD to develop, refine and publicize its "Risk Analysis and Management for Critical Asset Protection" (RAMCAP), which allows DHS to compare the vulnerabilities of disparate assets and resources against a series of benchmark threat scenarios. RAMCAP will enable DHS to allocate protective resources rationally, on the basis of risk.

B. *Specify the Roles and Responsibilities of Federal Agencies*

In December 2003, the President issued Homeland Security Presidential Directive 7, which clearly defines roles for various federal agencies in protecting the nation's critical infrastructure and key resources, and specifically names DHS as the lead or "sector-specific" agency for the chemical sector. With DHS's blessing, ACC organized the Chemical Sector Coordinating Council—a group of 16 leading trade associations that coordinates communications between DHS and our sector for purposes of infrastructure protection. ACC serves as the administrative secretariat for the Sector Council. This model has proven so attractive to DHS that they are encouraging its adoption by the other critical infrastructure sectors.

The federal Maritime Transportation Security Act (MTSA), which was enacted in late 2002, puts the Coast Guard in charge of regulating security within ports, on vessels, and at facilities that have the potential to be involved in a transportation security incident. Roughly 240 chemical plants in the United States—including most of the largest facilities nationally—are currently subject to rigorous Coast Guard oversight under the MTSA. These facilities have all conducted security vulnerability assessments, have implemented facility security plans, and have been inspected by the Coast Guard. Facility security plans specify actions the facility will take at different MARSEC (threat) levels regarding access control, restricted areas, handling cargo, delivery of vessel stores and bunkers, monitoring, security incident procedures, and barge fleeting facilities. They also include schedules for employee security training and response drills and exercises. Even more facilities are covered by area (i.e., port) security plans.

ACC supported the MTSA throughout the legislative process and we have worked closely with the Coast Guard to make the law a success. In particular, the U.S. Coast Guard recognized the Responsible Care® Security Code as an Alternative Security Program ("RCSC–ASP") for purposes of fulfilling facility security regulatory requirements under the MTSA. The RCSC–ASP was the first alternative security program the Coast Guard approved for facilities.

C. *Develop Appropriate Information Sharing Mechanisms*

Effectively securing privately-held infrastructure—like the business of chemistry—requires a partnership between the private sector and the government. Within seven months of 9/11, ACC and the FBI created a Chemical Sector Information Sharing and Analysis Center (ISAC) to share security information daily between the federal government and companies that make and use chemicals. The Chemical Sector ISAC provides 24–7 capability for DHS's Homeland Security Operations Center (HSOC) to contact the chemical sector as well as for individual members of the ISAC to convey incident or threat information to DHS. Members of the ISAC receive daily intelligence reports from DHS as well as episodic alerts and warnings. Open to any chemical sector business, whether or not it is a Council member, the ISAC has almost 600 participants. The Council runs the ISAC for free as a public service through its CHEMTREC service,[5] in cooperation with Department of Homeland Security (DHS). It is located at *http://chemicalisac.chemtrec.com.* ACC is also one of the first critical infrastructure sectors to be piloting DHS's new Homeland Security Information Network—Critical Sectors (HSIN–CS), a set of secure communications and collaboration capabilities. ACC anticipates that the Chemical Sector ISAC will eventually be integrated into HSIN.

On behalf of the chemical sector, ACC recently participated in TopOff 3, the third in a series of congressionally mandated emergency response exercises. TopOff 3 was the first such exercise to involve the private sector. ACC's involvement in TopOff 3 helped generate ideas for further improving the Chemical ISAC and added significant value to other signature parts of the exercise. The success of the public—private sector cooperation and coordination during TopOff 3 clearly underscored the value of private sector involvement, not only for providing expertise but ensuring

[5] CHEMTREC® is a 24-hour-a-day emergency communications center that ACC has operated as a public service since 1971. CHEMTREC® provides emergency responders with round-the-clock resources for information and assistance for spills, leaks, fires, explosions and other emergencies involving chemicals and other hazardous materials. CHEMTREC has provided critical information to emergency service workers for incidents ranging from the attacks at both the World Trade Center and the Pentagon to the Columbia space shuttle disaster.

that the business impacts of terrorist events and official reactions (or inaction) to such events are considered in both short and long term emergency management planning.

D. *Develop a Legislative Proposal*

ACC recognizes that not all chemical facilities are currently regulated under the MTSA. We also recognize that not all chemical facilities belong to ACC, and may not have taken the same kinds of aggressive steps that our members have taken—steps that have cost our members an estimated $2 billion since 9/11.

As a result, ACC has been taking a leadership role at the federal level to ensure that all chemical facilities are secured against the threat of terrorism. We have worked continuously with Congress and the Administration to secure enactment of national security legislation that will:

- Establish national standards for security of chemical facilities;
- Require facilities to conduct vulnerability assessments and implement security plans;
- Provide oversight, inspection, and enforcement authority to DHS.

In the absence of federal action on this vital topic, state legislatures are beginning to fill the vacuum. Both Maryland and New York have enacted chemical facility security laws. ACC was able to support both of these statutes, and is working with the two states' offices of homeland security on their implementation. However, we strongly believe a national program, not a patchwork of potentially conflicting state efforts, is necessary.

Naturally, ACC members feel that federal legislation should respect their substantial voluntary, at-risk expenditures implementing the Responsible Care® Security Code. As GAO's John Stephenson stated at April's Senate hearing: "I would expect that any federal system would give them credit for—indeed, recognize" ACC members' efforts. At the same hearing, Richard Falkenrath, former Deputy Homeland Security Advisor, concurred that these measures were "good," and that ACC member companies deserved "a level playing field" and "a common set of expectations" that all chemical facilities would be required to meet.

III. ACC's Views on Inherent Safety

In legislative and policy debates over chemical security, no issue has proven more controversial than the concept of "inherent safety" and what role it should play. Because of ACC members' deep investment in this issue, I would like to spend the balance of my time explaining our views and why we feel so strongly about them.

The concept of inherent safety was invented by the chemical engineering profession. In fact, it is no exaggeration to say that the business of chemistry, and indeed ACC members, wrote the book on inherent safety. The leading reference on the subject—*Inherently Safer Chemical Processes: A Life Cycle Approach,* also known as the "Gold Book"—was written by nine process safety experts, every one of whom worked for an ACC member company at the time.[6] The concept of inherent safety has been well understood within the process safety community for many years. Basically, it means designing a process to avoid creating a hazard in the first place, rather than trying to control the hazard afterward with add-on protective equipment or procedures.

The business of chemistry has long embraced inherently safer approaches. For over a decade and a half, our Responsible Care® initiative has required ACC members to have mechanisms for reviewing the design and modification of facilities and job tasks, with inherently safer design and material substitution at the top of the hierarchy of controls. This drives our members continually to develop and implement safer processes. We conduct process hazard analyses of our facilities, and those analyses can lead us to change processes, modify procedures, or substitute materials to reduce and manage risks. As I noted earlier, the Responsible Care Security Code mandates that our members take inherently safer approaches into account in assessing possible security measures. As a result, the GAO documented that seven out of the 10 ACC members it visited had made process changes as a part of their security enhancements.[7]

I cannot overemphasize, however, that inherent safety is about reducing all the risks potentially associated with a process. Inherent safety typically involves making very challenging risk/benefit judgments to ensure that risks are not unwittingly shifted or substituted, and that overall risks are reduced. Many inherently safer approaches involve trading one risk against the potential of another. For example, advocates of inherent safety frequently speak of reducing onsite inventories, or reduc-

[6] *Inherently Safer Chemical Processes: A Life Cycle Approach* (1996), published by the Center for Chemical Process Safety of the American Institute of Chemical Engineers.

[7] *See* "Protection of Chemical and Water Infrastructure," *supra* note 3, at 21.

ing or eliminating storage, of hazardous materials. By reducing inventories, though, a facility may increase the number of truck shipments through the plant's neighborhood. Similarly, replacing a low temperature, low pressure process that uses a toxic chemical with a process that uses a less toxic chemical, but operates at higher temperatures and pressure, could endanger workers.

Fundamentally, ACC has been dubious of any regulatory initiative that involves government agencies or other third parties reviewing and approving—or disapproving—facilities' decisions regarding inherent safety, whether in the context of security or otherwise. The history of "inherently safer" approaches is full of examples of unintended consequences: chlorofluorocarbons, underground storage tanks and PCBs were all originally regarded as inherently safer, from the perspective of fire or explosion. Their possible effects on stratospheric ozone, groundwater or health, however, were not fully appreciated until later.

The challenge to regulators is compounded by the complexity of chemical industry processes. There are no "standard processes" for making chemicals, and "[c]omplex process systems, especially those with a long history of safe performance, should not suddenly be changed without careful thought and consideration."[8] To expect effective regulatory oversight in this area is unrealistic, at least without great difficulty, expense and delay. In fact, in the Clean Air Act Risk Management Program rulemaking, EPA concluded that requiring and reviewing multiple process options at each regulated plant would not lead to greater advances in process safety.[9] In doing so, it recognized that no small, central group of people can be so omniscient as to be able to understand the huge range of issues involved at so many unique facilities.

The challenge facing regulators—and even businesses—is further heightened by that fact that, while the concept of inherent safety is well understood, how to implement that concept is not. One of the nation's leading academics in process safety has declared that "a systematic methodology to measure inherent safety does not exist, and it is not currently possible to know how inherently safe a plant or equipment item is because it is not possible to evaluate the principles that have been applied."[10] Another leading process safety expert concurs: given "the lack of formal and agreed inherent safety approaches . . . [e]xperience has shown that regulators and industry have a difficult time interpreting inherent safety and agreeing on adequacy of efforts."[11] This is not to say that such methodologies cannot be developed—they should, and ACC supports efforts to do so. But even if agreement on methods is achieved, leading process safety experts discount the feasibility of using them in a regulatory system: "[T]he complexity of process plants essentially prevents any prescriptive rules that would be widely applicable."[12]

Witnesses at April's Senate hearing agreed on the importance of legislation "focus[ing] tightly" on security and not becoming a "back door" way of addressing "extraneous" issues. Dr. Falkenrath maintained that the government should not have the power to order hazard reduction measures to be taken. Mr. Stephenson agreed, adding that many types of chemicals and chemical processes do not lend themselves to such approaches without massive capital expenditures, and that, in general, facilities using or storing such chemicals can make such changes more easily than manufacturing facilities.

In the final analysis, ACC firmly believes that judgments about inherent safety are fundamentally process safety decisions that must ultimately be left to the process safety professionals. We will remain concerned about legislation that would enable government officials focused on security to second-guess process safety decisions.

IV. Conclusion

In closing, I want to reiterate our commitments. Our member companies are committed to doing all they reasonably can to enhance the security of their operations and products against those who would do us harm. But we know that our nation

---

[8] David Moore, "Judging Effectiveness of Inherent Safety for Safety and Security of Chemical Facilities," presented at the 20th Annual CCPS International Conference (April 11–13, 2005), at 3.

[9] *See* 61 Fed. Reg. 31699 (June 20, 1996). Dr. Falkenrath testified before the Senate in April that he "disagrees" with those who would try to accomplish the goals of federal chemical security legislation through existing authority under the Clean Air Act's general duty clause, adding that it would be "politically imprudent" to accomplish such a significant intervention in the economy via such an indirect and imprecise mechanism.

[10] Sam Mannan, White Paper, "Challenges in Implementing Inherent Safety Principles in New and Existing Chemical Processes" (2002). Dr. Mannan is Director of the Mary Kay O'Connor Process Safety Center at Texas A&M University.

[11] David Moore, *supra* note 8, at 1.

[12] Mannan White Paper, *supra* note 10, at 6.

will not be safe until all chemical facilities that need to be protected have taken steps equivalent to those taken by our members.

It has been over three and a half years since 9/11. It is time to act, and we welcome this hearing. We are committed to working with you and others to see that legislation is enacted in this session of Congress. Thank you, and I'd be happy to answer any questions.

Mr. PEARCE. [Presiding.] Thank you for your testimony, and the Chair now recognizes Mr. Allen Summers, President and CEO of ASMARK, testifying on behalf of the Fertilizer Institute.

STATEMENT OF ALLEN SUMMERS

Mr. SUMMERS. Thank you, Mr. Chairman, members of the subcommittee. I am Allen Summers. I am a farmer, retail fertilizer dealer and a compliance consultant specializing in safety and security at agricultural retail locations. I am here today to testify on behalf of the Fertilizer Institute.

TFI is the leading voice of the Nation's fertilizer industry representing the public policy, communication and statistical needs of manufacturers, producers, retailers and transporters of fertilizer. On behalf of TFI, I very much appreciate the opportunity to testify today on the tremendous security efforts our industry has put forward.

We farm about 800 acres in Glendale, Kentucky. I also happen to be a co-owner of a retail farm center called Cecilia Farm Services in Cecilia, Kentucky. We do about a $5.7 million volume on an annual basis. We have a little over a thousand customers and we know who they are and call them by name when they walk through the door. We provide custom fertilizer each year for 30,000 of our customers' acres and we employ 8 full-time employees and 4 part-time employees.

In 1990, I founded the company called ASMARK to help our retailers in the country comply with the regulatory requirements. We are exclusively agriculturally based and our purpose is to assist the agricultural retailers with their DOT, EPA and OSHA compliance requirements. We have been in business a little over 15 years and lost only 4 clients. We have a very close industry, and I would like to paint you a picture of our typical facility. We are included in these chemical plants' security testimony today, but I need to paint you a very clear picture of our typical facility.

On average, the typical facility only has 5 to 7 employees. It is located in small, rural, sparsely populated communities, and we are really not attractive targets for terrorists. We are not a chemical facility, but we realize we do have a responsibility to secure our facilities. Our industry has already made a voluntary effort to secure our facilities.

Shortly after the September 11 tragedy, the fertilizer industry adopted a management practices security code designed to help the industry achieve continuous security performance using a risk based approach. The code calls on fertilizer makers to use methodologies developed by the Center for Chemical Process Safety or the Synthetic Organic Chemical Manufacturers Association when making security related improvements.

2002 also brought the year that we began work on a agricultural Web based security vulnerability assessment. We work with the Center for Chemical Process Safety to accredit the ASMARK's secu-

rity vulnerability assessment model. We work with the Fertilizer Institute, Agricultural Retailers Association, Crop Life America and the various State trade associations that we work with.

It was an industry collaboration, I might add, to make a Web based SVA available to the Nation's retailers. There is approximately 6,500 retailers of this description in our country. And to date, more than 2500 SVAs have been voluntarily performed around the United States. Other industry efforts include Clemson University recently purchased the SVA tool for use at 220 retail locations in South Carolina. The Alabama Department of Homeland Security has also expressed interest, and we are working with them now.

All facilities have developed and implemented written security plans required by DOT and the Coast Guard, and all facilities with anhydrous ammonia have prepared and implemented their risk management plan.

One addendum to my testimony I would like to make is that our facilities at a retailer are a program 2 RMPs and that may help the panel in their effort of assigning risk. I would also offer that our efforts to enhance security have been noticed by Congressman Ron Lewis as he introduced legislation to help offset some of the security related expenses in the form of a tax credit.

To conclude, we really don't consider ourselves a chemical facility and any legislation should be applied proportionately based on risk. Too many times our small industry gets saddled with one size fits all regulation that simply does not work and is not effective. We hope you will refrain from adopting antiquated concepts such as the inherently safer technologies which pose an economic and logistical threat to our industry.

All we ask is that our Members of Congress recognize the tremendous actions that have been taken in our small communities and by our small industry and provide fair treatment for low risk facilities such as our retailers.

I thank you for the opportunity to testify today and look forward to any questions you may have.

[The statement of Mr. Summers follows:]

PREPARED STATEMENT OF ALLEN SUMMERS

Introduction

Mr. Chairman and Members of the Subcommittee, I am Allen Summers. I'm a farmer, retail fertilizer dealer and compliance consultant specializing in safety and security at agricultural retail locations and I am here today to testify on behalf of The Fertilizer Institute (TFI). TFI is the leading voice of the nation's fertilizer industry, representing the public policy, communication and statistical needs of manufacturers, producers, retailers and transporters of fertilizer. On behalf of TFI, I very much appreciate the opportunity to testify today on the tremendous security efforts the American agricultural community has already undertaken and the steps Congress could take to bolster those efforts.

Currently, I reside in Owensboro, Ky., where I pursue my life-long commitment to agriculture, a commitment that began on my family's farm in 1974. We currently farm over 800 acres of corn, soybean, wheat and tobacco and raise beef cattle and hogs. I am also a partner in Cecilia Farm Service, a retail farm supply business located in Cecilia, Ky., which provides custom fertilizer and crop protection product application to over 1,000 customers, representing 30,000 acres with a dollar volume last year of $5.7 million. Cecilia has eight full time employees and hires four seasonal workers during the busy spring planting and fall harvest season.

Fifteen years ago I recognized a need in the agribusiness retail dealer community for assistance in bringing businesses into compliance with a wide range of federal

regulations. Subsequently, together with my wife Susan and business partner Randy Lawrence, I established ASMARK, Inc., which offers security and compliance assistance services regarding numerous regulatory regimes including: Department of Transportation (DOT) driver qualification requirements; the Environmental Protection Agency's Risk Management Program; and Occupational Safety and Health Administration hazard communication regulations.

Today, ASMARK, and its 14 full-time employees, is helping over 985 clients comply with federal regulations and meet industry security standards. Our clients include large, multi-outlet agribusiness retail dealers as well as smaller independent agribusinesses.

Fertilizer and Security

In response to the tragic events in Oklahoma City and the September 11 terrorist attacks, agribusiness retail dealers undertook tremendous efforts to ensure that criminals intent on harming our country could not purchase and misuse fertilizer and crop protection products that are vital in helping feed and nurture America and the world.

For example, in 2002 the fertilizer industry adopted a management practices security code designed to help the industry achieve continuous security performance using a risk-based approach. The code calls on fertilizer makers to use methodologies developed by the Center for Chemical Process Safety (CCPS) or the Synthetic Organic Chemical Manufacturers Association when making security-related improvements (* **Exhibit A**).

Also in 2002, I began working with several of my clients and the Agribusiness Security Working Group, comprised of members of TFI, the Agricultural Retailers Association and CropLife America, to develop a program to aid agribusiness retail dealers improve facility security to protect their fertilizer and crop protection products. As a result, a Web-based security vulnerability assessment (SVA) tool was developed and is now available to agribusiness retailers. The SVA tool is an invaluable security program that assists retailers in fully meeting the criteria the CCPS has created for conducting security vulnerability assessments (* **Exhibit B**). To date, the tool has proven to be a remarkable success, and is used by over 2,500 agribusiness retailers to develop security plans, based on SVA assessments, to address threats, risks and vulnerabilities.

The SVA tool also has a transportation component aimed at helping facilities comply with DOT security regulations. Most recently, Clemson University purchased the tool, making it available to all agribusiness retailers in South Carolina and just last week, I was contacted by the Alabama Department of Homeland Security regarding its potential interest in an arrangement to make the SVA available to all agribusinesses in Alabama. Naturally, we look forward to working with other states that might be interested in using the SVA to improve agribusiness facility security.

In addition to the Web-based SVA tool, the Agribusiness Security Working Group has also developed and widely distributed "Guidelines to Help Ensure a Secure Agribusiness." This six page document highlights three key security principles—identification of critical assets; establishment of layers of protection, and practice deter, detect and delay. The guidelines outline suggested practices covering facility security, customer transactions, special security measures and suggestions for partnering with customers on security and safety.

As an owner of a farm supply center and a farmer, I firmly believe I have an obligation to ensure the security of the chemicals I store and apply. For example, at my farm center local fire and law enforcement officials are frequently invited to walk through the facility to recommend what additional security measures might be needed and to be provided with updates on the types of products we have on hand. I cannot of course speak for everyone in the agricultural community, but I do know that many of us have, on a voluntary basis, installed expensive security upgrades, conducted background checks on our employees and complied with DOT security regulations for transportation. Without question, a great many members of the agricultural community have undertaken tremendous efforts to guarantee the security of our nation.

Across the country farmers and retailers are engaged in security efforts virtually unknown to the vast majority of the public. To illustrate, few members of the public may know that agricultural retailers and the Coast Guard work together to improve facility security. Yet from coast-to-coast, many agribusinesses have filed extensive security vulnerability assessments and plans with the Coast Guard in order to comply with the Maritime Transportation Security Act.

---

*Maintained in the Committee's File.

*Maintained in the Committee's File.

In addition, commodity and production agriculture groups are actively working with the U.S. Department of Agriculture to develop practices to better secure inputs and design bio-safety protocols to address farm and ranch security issues. These on-going efforts are intended to increase producer-level awareness of steps that can be taken to safeguard America from acts of terrorism.

What More Needs to Be Done?

During this hearing there has been considerable debate on whether Congress should approve chemical facility security regulations. There are those who charge that the chemical industry is not doing enough to secure products that wind up the hands of terrorists. In addition, there has been considerable debate over whether to mandate the use of inherently safer technologies (IST).

Mr. Chairman, at this time I would like to briefly comment on these issues. The agricultural community, which bears the great burden of producing the food that feeds the world, is totally committed to the security of our homeland. Our strong commitment to security can be seen in the many steps already taken to secure our facilities, our farms and our food supply. Animal and crop producers, and retailers across the country have voluntarily conducted security assessments and developed security plans in response. Through our national and affiliated state associations we continuously remind the agribusiness community of their obligations to secure their facilities and the products they handle. In short, the agricultural community has done so much to improve security and must receive credit for the voluntary actions we have already taken.

Mr. Chairman, it must be said that agribusinesses are generally located in rural, sparsely populated areas that are unlikely to be attacked by terrorists. The agriculture community has shown it is willing to do all that it can to help secure our country, but remember that each year millions of acres must be planted in a few short weeks and security measures that may work well for urban manufacturing centers will not work for agriculture. Therefore, it is essential that future security requirements are proportional to the risks found in rural communities.

Finally, IST is not a security issue—it is a safety issue. If there is a safer, more economical way of doing something, we do it. IST is a decades-old, antiquated concept that can only work when applied by a site owner's engineers who truly understand the operation of the facility. Any attempt to require IST by government edict jeopardizes worker and community safety. Mr. Chairman, the agriculture community would strenuously oppose any proposal that would mandate the use of IST.

Conclusion

Mr. Chairman and members of the committee, American farmers and retailers are committed to security, of that there can be no doubt. That commitment is readily demonstrated through the significant number of voluntary security steps our community has taken and will continue to take. Without question, we very much want to help Congress in its endeavors to shield this country from acts of terrorism. We support Department of Homeland Security (DHS) Secretary Chertoff's efforts to evaluate all of the nation's vulnerabilities and then prioritize the Federal government's response based on sound risk assessments.

All we ask is that members of Congress recognize the tremendous actions already taken by our community, provide fair treatment for small, low-risk facilities, and reject any and all attempts to revive obsolete concepts like IST. In taking on 21st Century terrorists, Congress must first recognize the progress that has been made to date and take account of on-going DHS efforts to develop a framework that recognizes the special needs of agriculture.

I thank you for the opportunity to testify today and look forward to answering any questions you might have.

Mr. PEARCE. Thank you, Mr. Summers, for your testimony, and the Chair now recognizes Mr. DePasquale, Security Specialist from the University of Georgia, to testify.

STATEMENT OF SAL DePASQUALE

Mr. DEPASQUALE. Mr. Chairman and Ranking Member Sanchez, if it is all right with the committee, you have my written statement and rather than read it to you in the interest of time to facilitate questions, if it is acceptable I certainly would waive reading it to you.

Mr. PEARCE. We have plenty of time to go ahead and you can make comments, and we have 15 minutes and 15 minutes legislatively could take us to next week.

Mr. DEPASQUALE. Thank you. My name is Sal DePasquale, and I have specialized in security for over 25 years with experience in chemical plants, industrial facilities, a range of government facilities, including the Department of Energy's facilities and many others. I thank the Chair for inviting me to speak with you today and allowing me an opportunity to share my observations relative to the security posture of chemical plants in our country and on the security of those industrial facilities that procure and utilize those chemicals.

Over the past 25 years, my career in security has provided me with an opportunity to view the industry from many vantage points as a security consultant, as a system design engineer, a corporate security manager and as an academician, which is with Georgia State University and not the University of Georgia. My comments today represent the cumulative span of my experience there.

There are three central points that I wish to make. The first is that although this is not the focus of this hearing, it is imperative, in my viewpoint, that consideration be given to the antagonisms that underlie the actions of our adversaries. To be sure, if the antagonisms are not addressed, the adversary will continue to attack, exploiting even the most remote vulnerabilities, taking greater risks and using bolder and more profound techniques for attack. The most thoughtful and comprehensive security programs may not be able to withstand the dedication of the adversary.

Even if the source of antagonism is diligently confronted, there is still a substantial need to address our degree of vulnerability. Today there is little resistance to an adversary using modest techniques for attack. Indeed, it may be argued that an inner city liquor store is better protected than are the facilities that manufacture and use highly toxic and lethal chemicals.

It is certainly true that we cannot inoculate ourselves against an attack, but surely we can do better than the mediocre and ineffectual practices that exist today. It is no secret that our industrial facilities are not prepared to defend against an armed assailant. Consequently, an adversary can reach a target using little more than a Saturday night special. Although industry claims it has invested considerably in security since September 11, the investments have been little more than window dressing. Indeed, the most sophisticated and costly camera systems cannot stop an armed assailant and may produce little more than material for use on the 11 o'clock news.

Substantive security upgrades will require the following: Construction of formidable property barriers, application of sophisticated intrusion detection systems, and deployment of a trained and properly equipped security force for response to prevent the adversary from reaching the target. In my viewpoint, anything less is simply to demonstrate some action, however ineffectual.

In a sense industry has been fortunate in that the adversary has used his skills to attack symbols of America. If the adversary alters strategy and attacks middle class America, industry may well be

the next element of commerce that will be transformed into a weapon.

Before we have a catastrophe that renders September 11 pale in comparison, I believe there are actions we may take to reduce our vulnerability to attack. I believe we need regulations. The legislation that was drafted by Senator Inhofe was rather promising. I would like to see it modified to require use of the physical security effectiveness tools produced by the Sandia National Laboratories, and I would like to see it include criminal penalties for corporate officers who fail to comply. In any event, I believe there are mechanisms available to avert a catastrophe, but it is imperative regulation provide the foundation.

Having worked with the American Chemistry Council and the American Institute of Chemical Engineers in developing guidelines, I am well aware of the industry's argument that it can regulate itself. However, I also know they are quick to say that they do not want to issue prescriptive standards and prefer the softer and gentler method of promulgating guidelines that do not require substantive action. In my estimation, if the industry will not issue substitute standards, it cannot say that it is self-regulating. It is simply a contradiction in terms.

The third point I would like to make is that it concerns emergency response preparedness. Across the country first responders have been scurrying to prepare for the threat of terrorism. That preparedness, however, has been couched within the paradigm of traditional exposures.

When I am teaching first responders, I ask them how prepared they are for a chemical event. Typically, the response is that they are making great progress. They will tell me that they have X number of people trained at technician level 1 and X number trained to technician level 2 and so on. I would then suggest to them that the training they described is aimed at industrial accidents, not a terrorist attack. Indeed, response training and response protocols are geared for industrial level accidents. First responders are trained to container release, to plug holes in a leaking vessel and such.

It is reasonable to project that a terror attack will not produce a leaking vessel, but instead will result in a ruptured vessel, completely unzipping the vessel. Within this context, there will not be any holes to plug. The magnitude of the release will quickly exceed the emergency response protocols and will likely result in injury to first responders.

The scenarios contemplated for upgrading preparedness are not consistent with what might be anticipated. Our first responder community needs to focus on protocols within the context of a terrorist attack.

Moreover, there is much lip service being paid to the new spirit of cooperation. At best, assorted agencies have conducted meetings to discuss the need for planning and then they go off individually and plan within the confines of their individual silo. It simply cannot go on that way if we are to be successful. In January of this year, in Graniteville, South Carolina, a railroad tanker carrying chlorine was involved in an accident.

Mr. PEARCE. If the gentleman would suspend there. If you could wrap up, we would appreciate it.

Mr. DEPASQUALE. In Graniteville, South Carolina, half the contents of a railcar was released and it was released over a 4-day period. Fortunately, it was in a sparsely populated region. The emergency management people who responded to that said we were fortunate, because if it was a densely populated area, the death toll would have been well into that 10,000 range, if not beyond.

Thank you.

[The statement of Mr. DePasquale follows:]

PREPARED STATEMENT OF SAL DEPASQUALE

Good afternoon Chairman Lungren, Ranking Member Sanchez, and Members of the Committee. My name is Sal DePasquale and I have specialized in security for over 25 years with experience in chemical plants, industrial facilities, a range of government facilities including Department of Energy facilities and many others.

I thank the chair for inviting me to speak with you today and allowing me an opportunity to share my observations relative to the security posture of chemical plants in our country and on the security of those industrial facilities that procure and utilize those chemicals.

Over the past 25 years my career in security has provided me with an opportunity to view the industry from many vantage points as a security consultant, a system design engineer, a corporate security manager and as an academician. My comments today represent the cumulative span of my experience.

There are three central points that I wish to make:

1. Although not the focus of this hearing, it is imperative that consideration be given to the antagonisms that underlie the actions of our adversaries. To be sure, if the antagonisms are not addressed, the adversary will continue to attack, exploiting even the most remote vulnerabilities, taking greater risks and using bolder and more profound techniques for attack. The most thoughtful and comprehensive security programs may not be able to withstand the dedication of the adversary.

2. Even if the source of antagonism is diligently confronted, there is still a substantial need to address our degree of vulnerability. Today there is little resistance to an adversary using modest techniques for attack. Indeed, it may be argued that inner city liquor stores are better protected than are the facilities that manufacture and use highly toxic and lethal chemicals.

> It is certainly true that we can not inoculate ourselves against an attack, but surely we can do better than the mediocre and ineffectual practices that exist today. It is no secret that our industrial facilities are not prepared to defend against an armed assailant. Consequently an adversary can reach a target using little more than a Saturday night special. Although industry claims it has invested considerably in security since September 11, the investments have been little more than window dressing. Indeed, the most sophisticated and costly camera systems can not stop an armed assailant and may produce little more than material for use on the 11 o'clock news.

Substantive security upgrades will require the following:

- Construction of formidable property barriers
- Application of sophisticated intrusion detection systems
- Deployment of a trained and properly equipped security force for response to prevent the adversary from reaching the target.

In my viewpoint, anything less is simply to demonstrate some action, however ineffectual.

In a sense industry has been fortunate in that the adversary has used his skills to attack symbols of America. If the adversary alters strategy and attacks middle class America, industry may well be the next element of commerce that will be transformed into a weapon.

Before we have a catastrophe that renders September 11 pale in comparison, I believe there are actions we may take to reduce our vulnerability to attack. I believe we need regulations. The legislation drafted by Senator Inhofe was rather promising. I would like to see it modified to require use of the physical security effectiveness tools developed by Sandia National Laboratories and I would like to see it include criminal penalties for corporate officers who fail to comply. In any event, I be-

lieve there are mechanisms available to avert a catastrophe, but it is imperative that regulation provide the foundation.

Having worked with the American Chemistry Council and the American Institute of Chemical Engineers in developing guidelines, I am well aware of industry's argument that it can regulate itself. However, I also know they are quick to say that they do not want to issue prescriptive standards and prefer the softer and gentler method of promulgating guidelines that do not require substantive actions. In my estimation, if the industry will not issue substantive standards, it can not say that it is self regulating. It is simply a contradiction in terms.

3. The final point that I wish to make concerns emergency response preparedness. Across the country first responders have been scurrying to prepare for the threat of terrorism. That preparedness, however, has been couched within the paradigm of traditional exposures.

When I am teaching first responders, I ask them how prepared they are for a chemical event. Typically the response is that they are making great progress. They will tell me that they have x number of people trained to technician level one and x number to level two and so on. I will then suggest to them that the training they described is aimed at industrial accidents, not a terrorist attack. Indeed, response training and response protocols are geared for industrial level accidents. First responders are trained to contain a release, plugging holes in a leaking vessel and such.

It is reasonable to project that a terror attack will not produce a leaking vessel, but instead will result in a ruptured vessel, completely unzipped. Within this context, there will not be any holes to plug. The magnitude of the release will quickly exceed the emergency response protocols and will likely result in injury to first responders.

The scenarios contemplated for upgrading preparedness are not consistent with what may be anticipated. Our first responder community needs to focus on their protocols within the context of a terror attack.

Moreover, there is much lip service being paid to the new spirit of cooperation. At best, assorted agencies have conducted meetings to discuss the need for planning and then they go off individually and plan within the confines of their individual silo. It simply can not go on this way, if we are to be successful.

In January this year, in Graniteville, South Carolina a railroad tanker carrying chlorine was involved in an accident that resulted in over half of its contents released into the atmosphere over a four day period. Two first responders and several residents were killed.

According to Georgia and South Carolina emergency management officials, the death toll could have been substantially higher. The area is sparsely populated and the material leaked out over several days. A massive rupture of a tanker in a highly populated area would produce a tragedy beyond imagination.

Although the accident was relatively contained, it is exemplary of the lethal potential of industrial chemicals.

Immediately after September 11, Senator Corzine and others put forth legislation to secure hazardous materials. The merits of the legislation may be debated, but it was an initial response to an obvious vulnerability. The chemical industry balked at the idea and argued that it could regulate itself more efficiently and effectively; ultimately killing the Corzine legislation.

The chemical industry regulates itself by way of the American Chemistry Council's Responsible Care program. This program includes guidelines for member companies to embrace to demonstrate responsible management of hazardous substances.

In regulating itself, however, the chemical industry says it does not want to produce prescriptive standards; it wants only to issue guidelines and best practices. It is very careful not to produce prescriptive standards for fear that the member companies might balk and because failing to comply with the standard would have legal implications.

Without prescriptive standards, however, there can be no self regulation. The result of guidelines and nice sounding best practices is to create a smoke and mirrors exercise that makes it appear that something serious is being accomplished, when it, indeed, is not.

The issue of security is no exception. In response to September 11, the ACC required its members to conduct a vulnerability analysis. This is a noteworthy exercise, but it does not require the companies to actually do anything in response to the analysis nor does it establish any minimum standards for defense against the most obvious exposures. Indeed, it is another exercise in smoke and mirrors; makes it seem like something substantive is occurring, when it is not. There are some additional requirements beyond the vulnerability analysis such as it is mandatory to have management support, but these additional items are innocuous.

Fundamentally, the standard should be sufficient security to withstand an attack by an armed adversary intent on using hazardous materials for mass casualties. As it is, an adversary with a six shooter can defeat the security of most facilities.

I thank you for this opportunity to testify, and I look forward to answering any questions you may have.

SAL DEPASQUALE ADDITIONAL STATEMENT

1. Law Enforcement and Security

There is a huge difference between Law Enforcement and Security, although the widespread paradigm is that they are synonymous; they are not. This does not mean a judgment that one is better than it other; it is simple to make a distinction.

Law Enforcement is skilled in enforcing the law, when the law has been violated. The skills include investigative practices, interogation techniques, crime scene analysis, evidence preparation, etc. Security is focused on risk analysis, identification of vulnerabilities, the technical aspects of security systems, barriers and response forces. These are very different skills.

When Homeland Security was formed, it was formed by combining numerous Law Enforcement agencies. The disarray that became evident after its commissioning was clearly demonstrated at the hearing last week. As the agency grappled with the tasks and responsibilities of security, it turned to the chemical industry, among others, for help in understanding chemical exposures. Industry lobbyists were all too willing to help. Consequently the agency provided data suggesting that a chemical attack would only expose about 10,000 people. In my estimation, this is astounding. You need look no farther than Bophal for an example of what may happen and, mind you, that event was not a complete vessel rupture.

I find this troubling because it seems the committee is looking to the agency and other experts to provide data upon which it can develop legislation, if need be. For the legislation to be sound and effective, it must be based on credible data. I would urge the committee to hear from credible sources on the consequences of a chemical attack; non partisan chemical engineers unaffiliated with the chemical industry. The emergency management officials who managed the chorine accident in Graniteville, South Carolina may also provide significant insight. U.S. military chemical warfare specialist may also provide quality data.

On the issue of how to secure dangerous chemicals I would suggest the committee hear from security officials from the Department of Energy, widely respected for their years of experience in security. The Homeland Security people claim they have helped the chemical industry by purchasing internet based cameras to aid in surveillance of the most sensitive chemical facilities. I would be very interested to hear the viewpoints of DOE security officials concerning the use of internet based cameras. My view is that this is terribly ill conceived as it allows the adversary to exploit internet security weaknesses to use the government purchased cameras for viewing the potentially targeted sites. Indeed, I would expect a junior security person to understand this fundamental tenant of security. Internet cameras have an application, but not where the stakes are high.

2. ACC reference to Third Party Verification

It was noted during the hearing that the American Chemistry Council's (ACC) security program includes third party verification of the security assessments conducted by member companies. It is important to understand what that means exactly. It may have changed since I was last involved with the ACC Security Guidelines, but as I understand it, the third party verification is limited solely to verifying that the company implemented the security measures that it thought it should implement. It is not a verification of the analysis and of the adequacy of the selected security measures.

This is analygous to a patient conducting a self diagnosis, discovering serious diseases and maladies, and concluding that they merely need some aspirin. The third party verifier simply needs to validate that the patient ingested the aspirin.

3. Security legislation should establish a credible agency with responsibilities for creating security codes and standards. The code should be similar to the fire code which accommodates a wide range of facilities and stipulates specific requirements.

The legislation should require the codes and standards be developed to address the following:

- Criteria for determining the chemicals requiring safeguards.
- Use of intrusion detection and physical barrier systems to detect and delay an adversarial attack.
- Security response capacity to intercept and immobilize the adversary before reaching the targeted chemical source.

- Use of analysis tools developed by Sandia National Laboratories for evaluation of the physical security effectiveness.
    - Estimate of Adversary Sequence Interruption (EASI)
    - System Analysis of Vulnerability to Intrusion (SAVI)
- Training and qualification criteria for security response officers.
- Background investigation criteria for individuals with access to the chemical source or chemical operations area.
- Protocols for investigation of suspicious activity
- Standards for security record keeping
    - Define classified data
    - Define public access data
- Standards for cyber security
    - Business management systems
    - Automated manufacturing production systems
- Requirements for periodic updating, modification and resubmittal of security plans for review and approval by the regulating agency.
- Requirements for submittal of security plans for review and approval by the regulating agency.
- Requirements for creating emergency response protocols.

Once again these are my viewpoints and not those of the organizations with which I am affiliated. Thanks again for the opportunity to express my views.

Mr. PEARCE. Thank you, Mr. DePasquale, and I thank all the witnesses. There are questions that the committee would like to ask, so with your indulgence, it will be about 15 to 20 minutes, and we will reconvene at the call of the Chair. The committee stands in recess.

[Recess.]

Mr. PEARCE. The committee will come to order and the Chair would recognize Mr. Dicks for questioning.

Mr. DICKS. Thank you, Mr. Chairman. We appreciate your efforts here to keep this going. Mr. DePasquale, is that how you say it?

Mr. DEPASQUALE. DePasquale.

Mr. DICKS. When you testified, you said we needed to have what kind of standards?

Mr. DEPASQUALE. Substantive standards that would give some specifics about establishing that barrier and establishing a response force that is capable of interceding and preventing the adversary from getting to the target. And I made reference to the models that have been developed by Sandia National Labs for evaluating physical security effectiveness, which are used in the Department of Energy and NRC environment extensively.

Mr. DICKS. What you are worried about is an armed group attacking one of these plants, and then once they get in they could then release these chemicals; isn't that basically the scenario you are talking about?

Mr. DEPASQUALE. That is correct. If I am an armed adversary and I use my weapon to eliminate whatever obstacle I have in front of me, an armed guard or whatever the case may be, and then I reach the target, which would be a vessel containing toxic materials, I place a bomb on it and unzip the vessel to release it.

Mr. DICKS. Now you also said that you have to have—trying to think of the phrase you used—substantive requirements and rather than just letting people self-regulate; if the industry will not issue substantive standards, it cannot say that it is self-regulating. It is simply a contradiction in terms.

Tell me what kind of substantive standards you think should be promulgated, either by Congress or by whoever.

Mr. DEPASQUALE. I would say that the standards should be to provide a response force that is capable and has the capacity to intercept and demobilize an adversary before the adversary reaches the target. And I would also suggest that part of that standard would be to use the tools developed by Sandia to evaluate the response force capability. I would establish a code and a database on physical security systems that establish the delay factors of each of those systems and the reporting times for the devices.

One of the mechanisms that Sandia has is it says if you have a fence and the fence has these devices on it, it will take an adversary 6 seconds to breach that barrier. And it will also evaluate other barriers that are between the exterior of the property and the target. And then what they evaluate is what is the response force capability. When you add up all the time that it takes the adversary to get through your obstacles, your physical security systems, is there sufficient time for the response force to be able to intervene?

Mr. DICKS. Mr. Durbin, do you have any problem with that?

Mr. DURBIN. Mr. Dicks, I think the way I would respond to that, our member companies through the Responsible Care Security Code did utilize vulnerability assessment methodology that was developed by Sandia National Labs as well as a separate one by the Center for Chemical Process Safety. I think the issue of having armed response, it is not necessarily an issue of whether you have full-time armed forces on site at every facility, but where appropriate, based on risk, based on your vulnerability assessment, is there an armed response capability that is nearby and dedicated. We have member companies across the range, not only the types of facilities that they operate, but the way they respond to—the types of guards or other forces they may have. Some will have full-time guards. Some of them are armed. Others work with the local law enforcement to ensure that there is a standard operating procedure, so if there is a rise in the threat level of some kind, they have an agreement with either local law enforcement, contract services, off duty folks, whatever it might be, to ensure that if there is a need at that facility, you will have that capability.

Mr. DICKS. That is not good enough, is it?

Mr. DEPASQUALE. No. The local police cannot get there quickly enough. The best local police response would not be—and I am not talking about every chemical facility, I am talking about facilities that have—

Mr. DICKS. You are talking about the ones that carry the highest risk?

Mr. DEPASQUALE. Exactly.

Mr. DICKS. We know the number of those. I think it is classified, but several hundred.

Mr. DEPASQUALE. I think there are many, many more. If I take one railcar of chlorine, that is 90 tons of chlorine, 90 tons. And there is a lot more than 123 of them. And if they are anywhere near a population, I am sorry, but I would venture to say that a lot more people are going to die than were characterized in those estimates that you heard earlier.

Mr. DICKS. Do you think Congress has to step in here and legislate in order to get this done?

Mr. DEPASQUALE. Actually, I think it is unreasonable to look at an industry association to expect it to come up with rigorous codes and standards that its membership is going to embrace and like. I don't think that that is plausible. When we look at traditional security practices, and as I look at many of the chemical facilities and industrial facilities, those practices are good for dealing with our traditional criminals. When we add into the equation a terrorist who wants to get at that material, that wants to cause massive death, that is a whole different thing.

Mr. DICKS. And willing to give up his life to do it?

Mr. DEPASQUALE. Willing to give up his life to do it. And it is just not tweaking the existing security. It is a radical rethinking of the security practices.

Mr. DICKS. Can we afford to do it? This is the other side of the equation. There are a lot of—this is one sector. We have 17 sectors. Now I do believe that because of the danger of some chemicals this has to be given special attention. But that is the other side of the equation.

Mr. DEPASQUALE. I don't mean to minimize that, because I believe the costs are substantial and formidable. I would say this. If I take the security posture of industrial America and I apply that same posture to Department of Energy facilities, I don't believe any of you would accept that. I believe that you would say there is no way we could allow our nuclear facilities to be protected like that. And I would suggest that when you look at the lethality of these materials it is not very much different.

Mr. DICKS. Thank you very much, and I appreciate your testimony. I am glad you were able to make your statement because I think it is a very important statement. Thank you.

Thank you, Mr. Chairman.

Mr. PEARCE. Thank the gentleman and the gentleman's time has expired. The gentleman from Massachusetts.

Mr. MARKEY. Mr. Durbin, you sent an e-mail to your corporate colleagues the same week that this committee marked up its Homeland Security authorization bill, and I would like to submit a copy, Mr. Chairman, of that e-mail for the record.

Mr. PEARCE: Without objection.

[The information follows:]

For Record Markey

-----Original Message-----
From: Freedhoff, Michal
Sent: Wednesday, June 15, 2005 10:38 AM
To: Freedhoff, Michal
Subject: FW: Chemical security materials

There is a lot of activity related to chemical security this week, so I want to be sure everyone has the attached materials for use in any meetings/calls/contact you have with Hill staff. The materials cover both facility and transportation security. I will send an update tomorrow morning on expected amendments, needed actions, etc., but below is a summary of what's going on this week legislatively. Please contact me with questions.

Actions this week:

1. Senate hearing in Homeland Security and Government Affairs Committee: Wed 4/27, 10am in SD-562. (Notice and witness list posted below). We have met, and will continue meeting with committee members to outline the actions ACC members have taken and the investments made in security since 9/11 without government direction, and are making sure they know ACC members SUPPORT meaningful, security-focused legislation. (See one-pager and RC fact sheet)

2. House Homeland Committee markup of DHS Authorization Bill: Wed 4/27, 10am in 2118 Rayburn. (They are marking up a committee print which is not yet available). The underlying bill does not address chemical security, but word is that Rep Ed Markey will offer a rail security amendment (his HR1414), and possibly a facility security amendment. We have asked everyone to contact members of the committee and urge them to reject the Markey amendments (Committee member list also attached).

3. Highway bill on the Senate floor: Senator Schumer and Senator Corzine may seek to offer their rail safety/security bills as amendments to the highway bill. Bill managers will attempt to table the amendments if offered. ACC has worked with coalition partners to provide talking points to committee staff. We are waiting for further intel/information to determine whether additional actions are necessary.

Materials:

(See attached file: one-pager 2-05.doc)(See attached file: RC Security Code-2004.doc)(See attached file: 2-1-05 stm.pdf)(See attached file: ACC and Transportation Security.doc)

Marty Durbin
Managing Director - Security & Operations Senior Director, Federal Relations
American Chemistry Council
703-741-5575

For Record Markey

U.S. Senate Committee on Homeland Security and Governmental Affairs

Title: Chemical Attack on America: How Vulnerable Are We?

Date: 4/27/05

Time (EST): 10:00 AM

Place: Dirksen Senate Office Building, Rm. 562

(Embedded image moved to file: pic10687.gif)

Witnesses

Panel 1

The Honorable Jon S. Corzine , Senator , United States Senate

For Record Markey

Panel 2

The Honorable Carolyn W. Merritt , Chairman and Chief Executive Officer , U.S.
Chemical Safety and Hazard Investigation Board

John B. Stephenson , Director, Natural Resources and Environment , U.S.
Government Accountability Office

Richard Falkenrath , PH.D. , Visiting Fellow, Foreigh Policy Studies , The
Brookings Institute

Stephen E. Flynn , PH.D. , Jeane J. Kirkpatrick Senior Fellow in National
Security Studies , Council on Foreign Relations

For Record Markey

Panel 2

The Honorable Carolyn W. Merritt , Chairman and Chief Executive Officer , U.S.
Chemical Safety and Hazard Investigation Board

John B. Stephenson , Director, Natural Resources and Environment , U.S.
Government Accountability Office

Richard Falkenrath , PH.D. , Visiting Fellow, Foreigh Policy Studies , The
Brookings Institute

Stephen E. Flynn , PH.D. , Jeane J. Kirkpatrick Senior Fellow in National
Security Studies , Council on Foreign Relations

Chemical Facility Security

Bottom Line: Members of the American Chemistry Council (ACC) are taking a leadership role to ensure that chemical facilities are secure from the threat of terrorism. We support national legislation that will:

- Establish national standards for security of chemical facilities;
- Require facilities to conduct vulnerability assessments and implement security plans;
- Provide oversight, inspection, and enforcement authority to the Department of Homeland Security to ensure facilities are secure against threats of terrorism.

Actions:

- Responsible Care® Security Code – mandatory for ACC members – has 4 basic components for facilities:
  - Prioritize facilities;
  - Assess vulnerabilities – methodologies developed by credible 3rd parties at Sandia National Lab and the Center for Chemical Process Safety (CCPS);
  - Implement security enhancements;
  - Verify physical enhancements.
- 2,040 ACC member facilities have completed rigorous vulnerability assessments and have implemented security enhancements;
- Since 9/11 ACC member companies spent more than $1 billion to further enhance security.

Q&A

Why does ACC support legislation?

- ACC members are doing the right thing and have set a benchmark for industry security programs. We need to ensure that all facilities – not just ACC members – are addressing security as rigorously as we do;
- We need to avoid a patchwork of laws at the state and local level – Maryland and New York have enacted legislation, while other states are considering proposals. *A national approach is more effective and appropriate;*
- Appropriate legislation will recognize and leverage the early, aggressive, and voluntary action already being taken by companies representing more than 90% of the productive capacity of the U.S. chemical industry. (We're NOT asking for an exemption: only that DHS determine if ACC's Responsible Care Security Code qualifies as an alternative compliance mechanism – just as was done with the Coast Guard port security regulations.)

February, 2005

American Chemistry Council Good Chemistry Makes It Possible

Fact Sheet

Responsible Care® Security Code

Contact: Jennifer Killinger, (703) 741-5833
Jennifer_Killinger@americanchemistry.com

October 1, 2004

Security has always been a top priority for America's leading chemical producers, and soon after the terrorist attacks of September 11, 2001, these companies took the lead in securing their facilities, a critical part of our nation's infrastructure. Without waiting for government direction, members of the American Chemistry Council quickly adopted the Responsible Care Security Code, an aggressive plan to further enhance security of our facilities, our communities and our products.

Under the Security Code – which addresses facility, cyber and transportation security – companies are required to conduct comprehensive security vulnerability assessments of their facilities, implement security enhancements, and obtain independent verification that those enhancements have been made. Implementing the Security Code under a strict timeline is mandatory for members of the American Chemistry Council and Responsible Care Partner companies. The Responsible Care Security Code has been widely recognized by local, state and federal governments as a model for other U.S. industries.

HOW THE RESPONSIBLE CARE SECURITY CODE WORKS

- **Prioritization and Assessment of Sites**
  Companies prioritize their facilities according to a four-tier system based on vulnerability. Security vulnerability assessments (SVAs) are then conducted at all facilities according to a schedule determined by the prioritization process.

- **Implementation of Security Measures**
  After completing the SVA process, companies implement security enhancements designed to control or mitigate the identified risks.

  - **Protecting Information and Cyber-Security** – Protecting information and process control systems is a critical component of sound security management and an essential part of the Security Code.

  - **Training, Drills and Guidance** – Emergency preparedness remains a hallmark of the Responsible Care initiative. Training, drills and guidance enhance security awareness and capabilities across the business of chemistry.

  - **Communications, Dialogue and Information Exchange** – Communications is an important part of the Security Code, which emphasizes cooperation among chemical producers, customers, suppliers, shippers and government agencies.

  - **Response to Security Threats and Incidents** – Companies evaluate, respond, report and communicate security threats as appropriate. Security incidents trigger a similar process with additional steps to conduct an investigation and take corrective action.

...more

ACC Fact Sheet
Responsible Care® Security Code

- **Continuous Improvement** – The Security Code includes planning, establishing goals and objectives, monitoring progress and performance, analysis of trends, and development and implementation of corrective actions.

- **Independent Verification** – Facilities undergo independent audits by third-party individuals and organizations to assure that they have implemented necessary security enhancements.

Through the Responsible Care Security Code, chemical companies have made and kept significant operational commitments. All Responsible Care facilities (more than 2000 nationwide) have completed rigorous security vulnerability assessments. The highest priority facilities (Tier 1) have already implemented security enhancements where appropriate, and the remaining facilities are on schedule to implement additional security measures by the end of this year. Full implementation of the Code will be completed by June 30, 2005. Timing for security vulnerability assessments, security enhancements and verifications is shown below.

	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Complete Facility Security Vulnerability Assessment	12/31/02 (Complete)	6/30/03 (Complete)	12/31/03 (Complete)	12/31/03 (Complete)
Complete Implementation of Facility Security Enhancements	12/31/03 (Complete)	6/30/04	12/31/04	12/31/04
Have Verification of Enhancements Completed	3/31/04 (Complete)	9/30/04	3/31/05	*

* Because Tier 4 facilities do not have potential offsite consequences, third-party verification is not required.

For more information on Responsible Care, visit: **www.ResponsibleCare-US.com**.

# # #

Statement

Contact: Kate McGloon (703) 741-5812
Kate_McGloon@americanchemistry.com

February 1, 2005

AMERICAN CHEMISTRY COUNCIL SUPPORTS FEDERAL LEGISLATION TO SECURE ALL U.S. CHEMICAL FACILITIES

(Arlington, VA) – The American Chemistry Council (ACC) today reiterated its longstanding support for federal chemical security legislation.

ACC member companies fully recognize that more work needs to be done to protect the nation's chemical sector and continue to urge the Administration and Congress to work together to enact security-focused legislation that will:

> establish national standards for security of chemical facilities,
> require facilities to conduct vulnerability assessments and implement security plans and provide DHS with oversight, inspection and enforcement authority.

The members of the ACC – representing approximately 90% of America's basic industrial chemical production – have spent more than $1 billion since 9/11 to make their communities, facilities and products more secure. Following 9/11, without waiting for government action, ACC members imposed on themselves a mandatory, comprehensive security program – ACC's Responsible Care® Security Code. As a result, all ACC member facilities have completed rigorous security vulnerability assessments and appropriate security enhancements and have nearly completed third-party verifications.

ACC's Security Code has been acknowledged by Secretary Ridge as a benchmark industry security program and has been recognized by the United States Coast Guard, the states of Maryland and New Jersey and the City of Baltimore.

Federal security legislation is necessary because chemical products are essential to the American way of life. They are used to make everything from safe drinking water and life-saving pharmaceuticals to computer chips and critical components for fighter aircraft. In addition, America's chemical makers employ nearly one million people in high-paying manufacturing jobs and export more products than any other industry.

Last spring, in comments marking the first anniversary of the Department of Homeland Security, President Bush said, "We're working with Congress on new legislation that establishes uniform standards for securing chemical sites and gives DHS the power to enforce those standards." ACC strongly encourages continued bi-partisan efforts in the 109th Congress to enact this much needed chemical security legislation.

# # #

http://www.accnewsmedia.com

The American Chemistry Council (ACC) represents the leading companies engaged in the business of chemistry. ACC members apply the science of chemistry to make innovative products and services that make people's lives better, healthier and safer. ACC is committed to improved environmental, health and safety performance through Responsible Care, common sense advocacy designed to address major public policy issues, and health and environmental research and product testing. The business of chemistry is a $460 billion enterprise and a key element of the nation's economy. It is the nation's largest exporter, accounting for ten cents out of every dollar in U.S. exports. Chemistry companies invest more in research and development than any other business sector. Safety and security have always been primary concerns of ACC members, and they have intensified their efforts, working closely with government agencies to improve security and to defend against any threat to the nation's critical infrastructure.

ACC AND TRANSPORTATION SAFETY & SECURITY

STRICT FEDERAL REGULATIONS -- All aspects of hazardous material transportation, including security, are covered by Department of Transportation hazardous materials transportation regulations. Such regulations include all modes of transport – truck, rail, maritime, air, and pipeline – and encompass identification and classification of hazardous materials, proper packaging, the provision of a 24-hour contact number and emergency response information that must accompany hazmat shipments, placarding and labeling, security planning, and training.

CHEMICAL INDUSTRY INITIATIVES – ACC members' commitment to continuous safety and security improvement has led to the development of a number of industry-specific programs.

1. Responsible Care®[1] -- Responsible Care is the U.S. chemical industry's award-winning performance initiative that has resulted in a 27% reduction in distribution incidents[2] among Responsible Care companies while chemical shipments increased 11% across the industry[3]. In the most recent reporting year (2001 – 2002) distribution incidents fell 18.3% among Responsible Care companies[2], while the volume of chemical shipments rose 2%.

2. Value Chain Due Diligence – As part of the continuous improvement commitment under Responsible Care, ACC members conduct comprehensive risk assessments and implement risk management to evaluate if, how, and with whom they will engage in business transactions. These risk assessments include considerations such as the mode of transportation, carrier performance, container design, consequences of a release, attractiveness of a vehicle as a terrorist target, and response resources available along the route, should an incident occur.

3. Training -- Every employee involved in the transportation of hazardous materials is required by federal regulation to undergo specific types of training relating to safety and security. Chemical companies have augmented those requirements with their own training programs.

4. Emergency Response -- Effective response systems, in addition to prevention measures, are key to safety and security. Chemical companies have created mutual response networks to bring to bear the best resources available to respond to those incidents. Additionally, the industry has instituted various public service programs, such as CHEMTREC® and the TRANSCAER® program, to assist public responders and local communities.

---

[1] http://www.responsiblecare-us.com

[2] Incidents involving hazardous material or hazardous waste reported by carriers to the Department of Transportation (DOT) on Form 5800.1, as required by DOT in 49 CFR 171.16.

[3] Based on the U.S. government's North American Industry Classification System (NAICS) 325. Includes inorganic and organic chemicals, synthetic materials, specialties, agricultural chemicals, pharmaceuticals, soaps and detergents, and other chemical products. Where company-specific data are not available, particularly in the area of economics, business of chemistry data are used to approximate Responsible Care companies. Responsible Care companies represent a sub-segment of the business of chemistry.

5. CHEMTREC® -- the Chemical Transportation Emergency Center – is a 24-hour-a-day emergency communications center that has been operated as a public service by the American Chemistry Council ("ACC") since 1971. CHEMTREC® provides emergency responders with round-the-clock resources for information and assistance for spills, leaks, fires, explosions and other emergencies involving chemicals and other hazardous materials. CHEMTREC has provided critical information to emergency service workers for incidents ranging from the attacks at both the World Trade Center and the Pentagon to the Columbia space shuttle disaster.

6. Transportation Security Guidelines[4] – Immediately after 9/11 ACC, in cooperation with CHEMTREC, the Chlorine Institute, the Compressed Gas Association and the National Association of Chemical Distributors, published ***Transportation Security Guidelines for the US Chemical Industry*** to address security considerations relative to the transportation of hazardous materials. The guidance generally applies to all modes of transportation (highway, rail, marine, air, and pipeline) and to the shipments of all hazardous materials, including chemical waste.

7. Responsible Care ® Security Code -Value Chain Security – In June 2002, the American Chemistry Council Board of Directors adopted the Responsible Care Security Code[5] as a condition of membership, requiring ACC members and Responsible Care Partners to implement a security management program in the areas of facility, value chain and cyber security. The Security Code consists of thirteen management practices, including vulnerability assessment, security enhancement, security preparedness and response policies and planning, third-party verification, management of change, and continuous improvement. Guidance for implementing the Security Code for a company's value chain was published September 2002.

PARTNERSHIP WITH OTHERS

1. TRANSCAER® -- The Transportation Community Awareness Emergency Response[6] program -- is a voluntary national outreach effort that links the chemical industry, transportation organizations and local emergency response services. ACC member companies and their partners in related industries – including railway and trucking companies – actively reach out to local communities, law enforcement agencies, and first responders to provide security and safety training, conferences, and other educational programs. TRANSCAER® members consist of volunteer representatives from the chemical manufacturing, transportation, distributor, and emergency response sectors, as well as the government that work through a network of regional and state coordinators. The TRANSCAER® program works with local communities to help them better understand the movement of hazardous materials and how to respond to a transportation incident should one occur.

2. Container Integrity – ACC members work closely with the railroads and railroad tank car manufacturers to review and improve the containers in which our products are shipped. Tank

[4] http://www.accnewsmedia.com/docs/300/250.doc?DocTypeID=4&TrackID=

[5] http://www.responsiblecaretoolkit.com/security.asp

[6] http://www.transcaer.org/public/home.cfm

car design criteria that are developed through these partnerships are also closely scrutinized by the U.S. Department of Transportation. In addition, the chemical industry is actively engaged with federal agencies and carriers in further research to explore how rail tank cars may be made even more resistant to terrorist attack.

3. Responsible Care® Partners – All large U.S. and Canadian railroads, as well as more than 50 other transportation service providers, are Responsible Care® Partners[7]. The Partnership Program extends the Responsible Care ethic beyond America's chemical product makers to their customers, carriers and others engaged in the business of chemistry. Together with the Partner companies, ACC members work to raise the standards of chemical operations and distribution. Partner companies must implement all relevant elements of Responsible Care, including those pertaining to distribution safety and security.

4. Homeland Security -- Security is a responsibility that is shared by both industry and government. ACC members work in partnership with federal security and law enforcement agencies to ensure that threat warnings are communicated clearly and quickly to chemical companies, carriers, and customers so that appropriate action may be taken. We have also established secure procedures for reporting suspicious activities to the Department of Homeland Security through the Chemical Sector Information Sharing and Analysis Center (ISAC)[8].

5. ACC/AAR Rail Security Task Force -- ACC teamed up with the Association of American Railroads (AAR) to identify additional ways to enhance the security of rail transportation and storage of chemical products. The two organizations, in conjunction with The Chorine Institute and the American Short Line & Regional Railroad Association, have produced guidance on communications, facility access, and security in transit.

[7] http://www.responsiblecaretoolkit.com/partners.asp

[8] http://chemicalisac.chemtrec.com/

Mr. MARKEY. In that e-mail you said that ACC members had told the Senate that the ACC supported Federal chemical security legislation, but said that ACC had asked everyone to tell the House to oppose the Markey Federal chemical security legislation. Now today, you are telling this subcommittee that you do support legislation, so I would like to understand exactly what it is that you do support.

Mr. Durbin, would the ACC support legislation that created mandatory enforceable risk-based Federal standards for chemical facilities that go beyond the voluntary measures that some ACC members have taken?

Mr. DURBIN. Yes, sir. That is what we have been saying all along. The Responsibility Care Security Code has set a model and we believe our members are doing the right thing, but we know it is not enough and that we need to make sure we have a national approach to ensure that all facilities that need to be protected are taking the same types of aggressive actions that our members have already taken.

Mr. MARKEY. Would the ACC support legislation that requires the Department of Homeland Security to evaluate chemical facilities security using force-on-force exercises by entities that are not, in fact, controlled by the security around the chemical facility?

Mr. DURBIN. That issue has not been discussed among ACC members. What I would suggest, if the regulations are done on a risk-based, performance-based process and that the vulnerability assessments required are done, you have a rigorous—

Mr. MARKEY. You are the Director of Security and Operations for the American Chemistry Council. Do you support having force-on-force tests of the security around chemical facilities?

Mr. DURBIN. I don't have enough information to be able to know whether that is appropriate.

Mr. MARKEY. You are the Director of Security?

Mr. DURBIN. Yes.

Mr. MARKEY. You don't have a view on whether or not force-on-force—

Mr. DURBIN. I believe if the regulations are developed in a risk-based manner and it is determined—and again, we have said that we should give authority to the Department of Homeland Security to develop the regulations. And in that process, they determine that—

Mr. MARKEY. I am asking your view. I am not asking for their view. You are the expert witness. Do you believe that force-on-force tests of existing security around chemical facilities is something that we should include?

Mr. DURBIN. I think it should be considered.

Mr. MARKEY. But not included?

Mr. DURBIN. I don't have enough expertise.

Mr. MARKEY. I have a hard time believing that the Director of Security for the chemical industry has no view on that critical question. There are only three or four critical questions. And you don't have a view?

Mr. DURBIN. I would be more than happy to get back to you on that.

Mr. MARKEY. Would the ACC support legislation that required companies to reduce the risks their facilities posed by taking steps to replace toxic chemicals or processes with less dangerous technologies when it is economically and technologically feasible for them to do so?

Mr. DURBIN. No, sir. We would not, but I want to make clear that we believe the issue of—as you are doing your vulnerability assessments and security plans as within the Responsible Care Security Code, you absolutely would have to consider inherently safer design approaches. And frankly ACC member companies have been required to do that under the Responsible Care program even prior to the security code. That continues to be a core part of the way our member companies do their business, always searching for inherently safer ways of making their products and moving their products. And if you are doing a vulnerability assessment, a rigorous vulnerability assessment, that helps you identify areas where you can make process changes.

Mr. MARKEY. That is an honest response. Would the ACC support having whistleblower protections for anyone who is retaliated against for reporting chemical security flaws that match at least the protections which the Sarbanes–Oxley Act provides for whistleblowers when they turn in bad corporate practices at private firms?

Mr. DURBIN. I believe so. Again, that is not an issue we specifically discussed within ACC. I know those types of protections have been included in proposals that have been made and that has not been one of the areas where we have had any concerns.

Mr. MARKEY. In your testimony, you state that your member companies have taken steps to incorporate ACC's best practices. Has ACC attempted to visit all of these companies to verify that they have done so?

Mr. DURBIN. Not ACC itself. We are a trade association and not an enforcement agency. Our member companies had third parties come in themselves from the local area to verify that physical security enhancements were made at facilities.

I would like to make one other thing clear. ACC has not taken the position that we should be left alone or we are self-regulating. What we have said is we have set a bar on what needs to be done in security and that we believe there is a need for national legislation to ensure that the entire chemical sector is protected.

Mr. MARKEY. Mr. DePasquale, as you know, the chemical industry has opposed all legislative proposals that contain a requirement to switch to less dangerous technologies in order to reduce the risk. In fact, Mr. Durbin's testimony today restated that point. In your opinion and based on your extensive industrial experience, have chemical companies already done everything they can to switch to safer chemicals, processes in order to reduce the risk to their facilities?

Mr. DEPASQUALE. You know, it is a curious thing. I have had several instances where I had a facility that used chlorine and they had examined prior to my involvement with them on a security issue, they had examined the feasibility of changing to other materials that were inherently safer, not completely safe, but still not as volatile as chlorine was. And they looked at the cost, number one, from a capital expenditure, and secondly from the ongoing ex-

pense, and it was a difficult management decision to make. When we brought into play the security issues, those were the things that in many cases drove them to say there is an added reason why we should do this, and they did.

So, yeah, I think there are industries out there who will be responsive. And I also think that in terms of the legislation that if I have to comply with these things if I am using these materials, implied in it is if I am not using those materials then I don't have to comply with these regulations. So it seems to me that it is a fairly straightforward decision for companies to make.

Mr. MARKEY. Mr. Chairman, I have one final question and I appreciate your indulgence, and that is to you, Mr. Summers. As you know, the bomb that Timothy McVeigh used to kill 168 was made with 2 tons of ammonium nitrate used in fertilizer. So was the 1993 World Trade Center bomb. The October, 2002 Al-Qa'ida attack on a Bali nightclub also reportedly used ammonium nitrate. Last year 3,000 pounds of ammonium nitrate was stolen from a fertilizer plant in North Carolina. In your testimony, you stated that many fertilizer and other agribusinesses have voluntarily increased security.

Do you agree that facilities that manufacture or store significant quantities of ammonium nitrate should be required to increase security to ensure that it can't be stolen or detonated on site by terrorists?

Mr. SUMMERS. Well, I can't speak for everybody. My opinion is that the requirements of anything that is considered by the Department of Homeland Security should be a risk-based approach, and obviously someone that manufactures ammonium nitrate and someone who sells a pallet of it or stores a ton of it in a bulk building is two entirely different scenarios. One size fits all does not apply to our industry. So we would like differentiation between that.

Mr. MARKEY. And where would you accept that top security is necessary?

Mr. SUMMERS. Being in the regulatory consulting business, there are some categories. And one of the things I heard today, I heard that there was 15,000 risk management plant facilities in the United States. One thing that I also heard was that there was not a good understanding. Mr. Stephan with the Department of Homeland Security tried his best to describe that worst case scenario and the prevailing winds, and I think there is an understanding that needs to be gained along that line that would help.

In the RMP program there is program 1, which is a pretty insignificant hazard. There is a program 2 RMP that is probably easier to explain by explaining program 1 is an insignificant hazard. Program 3 is the most significant hazard. And program 2 categorizes everyone that doesn't fit in program 1 and program 3. And our retail facilities fall into program 2 RMPs. If I had to suggest something as Allen Summers from ASMARK, a farmer, retailer and consultant, I would say risk management plan 2 and 1 are categories that probably don't pose a huge risk.

There has been testimony today that said that 10,000 people would be affected—10,000 lives could be lost and 40,000 people could be affected within that area of concern around the plant at

one of the worst facilities and one of the most highest risk facilities in the country. We work approximately 34 percent of our facilities of the 985 that we work with have anhydrous ammonia. They are all program 2 risk management plans. And 99 percent of those, I can't give you definite numbers, but 99 percent of those have less than 250 people in that 1.2 or 2.7-mile area of concern around the plant. We are not talking about significant risk here.

Mr. MARKEY. I want to get through this. How much ammonium nitrate was necessary to blow up the World Trade Center? They tried in 1993 and left a huge hole there. And the same thing is true for the Murrah building in Oklahoma City. What category would you put that in, the amount of ammonium nitrate in those two instances? What category would you—

Mr. SUMMERS. While I am appearing here today in defense of our industry and hoping that trying to describe what we have done and the money we have spent and the actions we have taken in doing our own security vulnerability assessment working and creating that methodology with the Center for Chemical Process Safety—

Mr. MARKEY. Do you agree—and I apologize, Mr. Chairman—but do you agree that Al-Qa'ida has ammonium nitrate at the top of its terrorist target list given what they did in Bali and what they did at the World Trade Center?

Mr. SUMMERS. No, I don't necessarily agree with that. There are a lot more attractive targets in the United States than that.

Mr. MARKEY. Unfortunately, two of the biggest instances did involve ammonium nitrate, so we have to take note of that in committee in terms of the amount.

Mr. SUMMERS. If I could finish in answering your first question. While I am here today defending our industry and saying there needs to be risk based assessment applied to this decision, in the days to come, there is going to be—as an industry, we already recognize that we need to regulate the sale of ammonium nitrate and there will be a bill introduced.

Mr. MARKEY. What I am trying to get from you so the committee could have the expertise—

Mr. PEARCE. The gentleman's time has expired.

Mr. MARKEY. How much volume do you think requires that kind of security?

Mr. SUMMERS. I am not qualified to speak for the industry, but Allen Summers' opinion is that in order to do it we probably need to regulate every bag.

Mr. PEARCE. Gentleman's time has expired. And anyone else on the committee who seeks recognition? The chairman recognizes himself for 5 minutes.

Mr. Bandy, are you aware of any of the regulations regarding EPA and the voluntary compliance mechanism that they have for different companies? The reason I ask is that Marathon has been recognized as one of the companies nationally that EPA has given full oversight of its own processes, and they come in periodically and check. And it just is a new paradigm in the last 5 years, I suspect, that EPA has engaged in.

Mr. BANDY. That is EPA performance track. I am not familiar with the details.

Mr. PEARCE. Do you think that those same parameters could come into play in this particular arena?

Mr. BANDY. Yes, I do. And OSHA has a similar program, voluntary protection program where they come in and evaluate your facility every 3 years.

Mr. PEARCE. Mr. DePasquale, as far as the ammonium nitrate, do you think—you said we should radically rethink our security. Can we secure our facilities to keep the theft of ammonium nitrate from occurring in your radical rethinking?

Mr. DEPASQUALE. I believe we can. One of the issues—

Mr. PEARCE. If we assume that we can, how would you handle the fact that someone who wants to blow up the World Trade Center, the purchase really—would you control the purchases, too?

Mr. DEPASQUALE. Right now it is relatively easy to purchase not only ammonium nitrate but other explosives as well.

Mr. PEARCE. Even if it were difficult, the cost and the regulatory effect, is there a radical rethinking that can protect us from that, yes or no?

Mr. DEPASQUALE. Radical rethinking, yes.

Mr. PEARCE. You could envision in your experience a radical rethinking that could keep anyone from purchasing a controlled substance and putting it to use against us?

Mr. DEPASQUALE. I don't think I would go that far. There is always a way for people to still breach—

Mr. PEARCE. That might be my point, Mr. DePasquale. Even a radical rethinking, we have to evaluate the cost to us as a nation and the cost to our freedoms.

A great, great dishonor has been done to you, my friend. I apologize. Anytime—as a graduate from a State university, anytime I would be declared to be a graduate from the University of New Mexico rather than New Mexico State, I would feel a deep, deep wound. And so I apologize that this committee has declared you to be from the University of Georgia, and we will create that in the testimony and in the written testimony.

All of you have been very patient. We appreciate your testimony. It is a very difficult subject and the answers—

Mr. MARKEY. Mr. Chairman, could I ask one more question?

Mr. PEARCE. No, Mr. Markey. Your time has elapsed.

Mr. MARKEY. May I ask unanimous consent?

Mr. PEARCE. The unanimous consent is not agreed to, because the chairman objects.

Mr. MARKEY. Can I make a parliamentary inquiry?

Mr. PEARCE. Mr. Markey, you may not.

Mr. MARKEY. Mr. Chairman, I think you have to allow a parliamentary inquiry.

Mr. PEARCE. You can make the parliamentary inquiry. Is it required that the witnesses be present for this? I would ask counsel if we can—you are bound to stay. The hearing is not over, you are still here. I apologize. And we will sit here until southern New Mexico freezes over if necessary to hear this necessary parliamentary inquiry.

Mr. MARKEY. The parliamentary inquiry just goes to the issue of the fact that no other members came back from the vote on the floor. The witnesses are here. It is late and I just have another

question to ask. And from a parliamentary perspective, I am asking the Chair why he would object to an additional question being asked.

Mr. PEARCE. Thank you. The Chair would point out that the gentleman had 5 minutes and the Chair allowed an additional 7 minutes. About 5 of that elapsed after the gentleman reported that he had one more question, at which point there were multiple questions asked.

I think the Chair has been very sensitive to the needs of the gentleman to ask questions to take advantage of the presence of these witnesses who have great, great knowledge on the issues. I think the chairman has given the gentleman ample opportunity to express his questions even to recognizing the gentleman before anyone on the majority side. I am not sure exactly why at 6:20 in the evening the gentleman would like to hold our witnesses for another round of questioning. But in response to that, I am willing to sit here and discuss the parliamentary inquiry at full length and the full breadth and would be willing to answer all questions that the gentleman has for me even at the delaying of our witnesses.

So again, the Chair would make himself available to the parliamentary inquiry.

Mr. MARKEY. I thank the gentleman. From a parliamentary perspective, as the gentleman knows that the hearing was supposed to start at 2:00 and, although the witnesses had no control over it, we then had eight roll calls that were called by the—on the floor of the House. And then subsequently, we had just another three roll calls. And there is no issue more critical to the security of our country, and of course the witnesses did not schedule 2:00 on a Wednesday afternoon for the hearing. So they are blameless in this. But obviously, the fact that we had between 10 and 11 roll calls in that brief period of time has reduced dramatically, as you can see from the attendance of the membership who came back after the witnesses finished their testimony. So no one actually came back with the exception of me and you, Mr. Chairman, who asked questions along with Mr. Dicks.

Mr. PEARCE. There was one Democrat.

Mr. MARKEY. As I said, along with Mr. Dicks.

Mr. PEARCE. I missed that you included Mr. Dicks in the listing there.

Mr. MARKEY. And the point I am making is that this is the panel on the subject. And unfortunately, because of circumstances beyond their control, although they probably came to this city at great expense, that members can't come because of the White House picnic where many of them are right now, but the experts on this subject are here with a willingness to answer questions from the panel. I don't hear any request from them they have to leave. I am pointing that out from a parliamentary perspective of where we are at this point. It is not their fault. It is not the member's fault or your fault. It is what happens when you schedule something at 2:00 in the afternoon and have 10 roll calls that you still have this panel here on an historic day where the American chemical industry has changed its position and we have an excellent opportunity to continue to explore that.

But I can understand—I can sense an intransigence in the chairman's voice and I appreciate that, and it is your prerogative as the chairman to deny any further questions. And it appears that you are going to exercise that prerogative. Given the totality of the circumstances, we would be better off to continue to use the expertise of this perhaps one-time gathering on the experts of chemical security in America.

And I yield back the balance.

Mr. PEARCE. I thank the gentleman for yielding. Are their observations from the witnesses? Any time you would like to elapse on your own now? Having said that, the hearing will now be adjourned.

Thank you.

[Whereupon, at 6:30 p.m., the subcommittee was adjourned.]

○