

COMBATING TERRORISM: CHEMICAL PLANT SECURITY

HEARING

BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS AND INTERNATIONAL
RELATIONS

OF THE

COMMITTEE ON
GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

FEBRUARY 23, 2004

Serial No. 108-156

Printed for the use of the Committee on Government Reform



Available via the World Wide Web: <http://www.gpo.gov/congress/house>
<http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

94-257 PDF

WASHINGTON : 2004

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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana	HENRY A. WAXMAN, California
CHRISTOPHER SHAYS, Connecticut	TOM LANTOS, California
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
JOHN L. MICA, Florida	PAUL E. KANJORSKI, Pennsylvania
MARK E. SOUDER, Indiana	CAROLYN B. MALONEY, New York
STEVEN C. LATOURETTE, Ohio	ELIJAH E. CUMMINGS, Maryland
DOUG OSE, California	DENNIS J. KUCINICH, Ohio
RON LEWIS, Kentucky	DANNY K. DAVIS, Illinois
JO ANN DAVIS, Virginia	JOHN F. TIERNEY, Massachusetts
TODD RUSSELL PLATTS, Pennsylvania	WM. LACY CLAY, Missouri
CHRIS CANNON, Utah	DIANE E. WATSON, California
ADAM H. PUTNAM, Florida	STEPHEN F. LYNCH, Massachusetts
EDWARD L. SCHROCK, Virginia	CHRIS VAN HOLLEN, Maryland
JOHN J. DUNCAN, Jr., Tennessee	LINDA T. SANCHEZ, California
NATHAN DEAL, Georgia	C.A. "DUTCH" RUPPERSBERGER, Maryland
CANDICE S. MILLER, Michigan	ELEANOR HOLMES NORTON, District of Columbia
TIM MURPHY, Pennsylvania	JIM COOPER, Tennessee
MICHAEL R. TURNER, Ohio	_____
JOHN R. CARTER, Texas	_____
MARSHA BLACKBURN, Tennessee	_____
_____	BERNARD SANDERS, Vermont
_____	(Independent)

MELISSA WOJCIAK, *Staff Director*

DAVID MARIN, *Deputy Staff Director/Communications Director*

ROB BORDEN, *Parliamentarian*

TERESA AUSTIN, *Chief Clerk*

PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL
RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MICHAEL R. TURNER, Ohio	DENNIS J. KUCINICH, Ohio
DAN BURTON, Indiana	TOM LANTOS, California
STEVEN C. LATOURETTE, Ohio	BERNARD SANDERS, Vermont
RON LEWIS, Kentucky	STEPHEN F. LYNCH, Massachusetts
TODD RUSSELL PLATTS, Pennsylvania	CAROLYN B. MALONEY, New York
ADAM H. PUTNAM, Florida	LINDA T. SANCHEZ, California
EDWARD L. SCHROCK, Virginia	C.A. "DUTCH" RUPPERSBERGER, Maryland
JOHN J. DUNCAN, Jr., Tennessee	JOHN F. TIERNEY, Massachusetts
TIM MURPHY, Pennsylvania	_____
_____	_____

EX OFFICIO

TOM DAVIS, Virginia	HENRY A. WAXMAN, California
LAWRENCE J. HALLORAN, <i>Staff Director and Counsel</i>	R. NICHOLAS PALARINO, <i>Senior Policy Advisor</i>
ROBERT A. BRIGGS, <i>Clerk</i>	

CONTENTS

	Page
Hearing held on February 23, 2004	1
Statement of:	
Liscouski, Robert P., Assistant Secretary of Homeland Security for Infrastructure Protection, Department of Homeland Security; Robert Full, chief, Allegheny County Department of Emergency Services; and Thomas W. Headley, vice chairman, Forward Township Board of Supervisors	8
Stephenson, John, Director of National Resources and Environment for the U.S. General Accounting Office; Pamela Witmer, president of the Pennsylvania Chemical Industry Council; Marty Durbin, team leader for security and operations and senior director of Federal relations for the American Chemistry Council; and Jennifer C. Gibson, vice president of government and public affairs, National Association of Chemical Distributors	50
Letters, statements, etc., submitted for the record by:	
Durbin, Marty, team leader for security and operations and senior director of Federal relations for the American Chemistry Council, prepared statement of	84
Full, Robert, chief, Allegheny County Department of Emergency Services, prepared statement of	18
Gibson, Jennifer C., vice president of government and public affairs, National Association of Chemical Distributors, prepared statement of ...	105
Headley, Thomas W., vice chairman, Forward Township Board of Supervisors, prepared statement of	22
Liscouski, Robert P., Assistant Secretary of Homeland Security for Infrastructure Protection, Department of Homeland Security, prepared statement of	11
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3
Stephenson, John, Director of National Resources and Environment for the U.S. General Accounting Office, prepared statement of	53
Witmer, Pamela, president of the Pennsylvania Chemical Industry Council, prepared statement of	76

COMBATING TERRORISM: CHEMICAL PLANT SECURITY

MONDAY, FEBRUARY 23, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING
THREATS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:30 a.m., at Moon Township Municipal Building, Auditorium, 1000 Beaver Grade Road, Moon Township, PA, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Murphy, Shays and Turner.

Staff present: Lawrence Halloran, staff director and counsel; R. Nicholas Palarino, Ph.D., senior policy advisor; and Robert A. Briggs, clerk/policy analyst.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats and International Relations hearing entitled, "Combating Terrorism: Chemical Plant Security," is called to order.

Let me first thank Congressman Tim Murphy for inviting the subcommittee here today. He is a thoughtful, active participant in our oversight, and we are happy to have the opportunity to examine the important issue of chemical plant security from this perspective. I will be turning over the chairmanship once we've sworn in our first panel, and he'll conduct the rest of the hearing.

According to a February bulletin from the Department of Homeland Security [DHS], National Infrastructure Protection Center, industrial chemical plants remain "viable targets" for attacks by al Qaeda terrorists. So we meet this morning to ask if the public and private sectors are pursuing an equally viable strategy to repel or respond to those attacks.

Many in this area may not think so, and for good reason. Through last year, a series of media reports pointed to chronically lax security and obviously avoidable vulnerabilities at chemical facilities here and across the Nation. A porous perimeter of fallen fences and poorly aimed security cameras that failed to stop intruders armed only with pens and cameras is not likely to deter trained terrorists seeking access to deadly chemicals.

What is at risk? More than 15,000 U.S. facilities use large amounts of extremely hazardous substances; 3,000 of those sites project worst-case hazardous zones in which released chemicals could reach more than 10,000 people nearby or far downwind. Vul-

nerability zones around 125 chemical plants could each encompass more than 1 million people.

Securing this widely dispersed network of chemical production, storage and distribution facilities poses difficult challenges and demands tough choices. Given the undeniable attractiveness of toxic and flammable compounds terrorists could use as prepositioned weapons of mass destruction, the need for increased physical security is obvious. But gates, guns and guards are not the only answers. Chemical infrastructure could remain economically critical, but less vulnerable, if inherently safer substances and processes were adopted to reduce their toxic utility to terrorists. Increased security and reduced chemical risk need not be mutually exclusive, but so far sustained progress on either seems much too elusive.

Another challenge posed by increased chemical facility security pits the need for public information and awareness against the effort to keep facility plans and strategies out of the hands of terrorists. Documents on emergency response plans and chemical plant preparedness have been removed from the Internet and other public sources. The question remains whether that loss of transparency enhances security more than it shields poor planning from needed public security.

As in other areas of terrorism preparedness, the chemical industry and those who regulate it are hard pressed to answer the question, "Prepared for what?" Without threat-based standards against which to measure security spending, money and time are being wasted lurching from crisis to crisis, as each code orange alert and sensational media incursion highlights new vulnerabilities.

The Department of Homeland Security is conducting an inventory of America's critical infrastructure in formulating preparedness standards to secure key industrial targets from terrorists. The Assistant Secretary of DHS for Infrastructure Protection, Mr. Robert Liscouski, will testify on the status of those efforts. We obviously appreciate him being here today.

State and local officials, industrial association representatives and an expert from the U.S. General Accounting Office will also testify. We appreciate the time, dedication and expertise of all our witnesses, and we look forward to their testimony.

[The prepared statement of Hon. Christopher Shays follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN
DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
LEANA ROS-LEVENSON, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
EVEN G. LATOURETTE, OHIO
DICK CISE, CALIFORNIA
JIM LEWIS, KENTUCKY
T. ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN EL CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

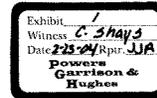
MAJORITY (202) 225-6274
FACSIMILE (202) 225-3974
MINORITY (202) 225-6261
TTY (202) 225-6602

www.house.gov/reform

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2546
Fax: 202 225-2382
GROC NS@mail.house.gov
<http://www.house.gov/reform/ns/>

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDCOLPHUS TOWNS, NEW YORK
PAUL E. KANZISKO, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
W. LACY GLAY, MISSOURI
DANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT



Statement of Rep. Christopher Shays
February 23, 2004

Let me first thank Congressman Tim Murphy for inviting the Subcommittee here today. He is a thoughtful, active participant in our oversight, and we are happy to have the opportunity to examine the important issue of chemical plant security from this perspective.

According to a February bulletin from the Department of Homeland Security (DHS) National Infrastructure Protection Center, industrial chemical plants remain "viable targets" for attacks by Al Qa'ida terrorists. So we meet this morning to ask if the public and private sectors are pursuing an equally viable strategy to repel or respond to those attacks.

Many in this area may not think so, and for good reason. Through last year, a series of media reports pointed to chronically lax security and obviously avoidable vulnerabilities at chemical facilities here and across the nation. A porous perimeter of fallen fences and poorly aimed security cameras that failed to stop intruders armed only with pens and cameras is not likely to deter trained terrorists seeking access to deadly chemicals.

More than 15,000 U.S. facilities use large amounts of extremely hazardous substances. Three thousand of those sites project worst-case hazard zones in which released chemicals could reach more than ten thousand people nearby or far downwind. Vulnerability zones around one hundred and twenty-five chemical facilities could each encompass more than one million people.

Securing this widely dispersed network of chemical production, storage and distribution facilities poses difficult challenges and demands tough choices. Given the undeniable attractiveness of toxic and flammable compounds terrorists could use as pre-positioned weapons of mass destruction, the need for increased physical security is obvious. But gates, guns and guards are not the only answers. Chemical infrastructure could remain economically critical, but less vulnerable, if inherently safer substances and processes were adopted to reduce their toxic utility to terrorists. Increased security and reduced chemical risk need not be mutually exclusive. But so far, sustained progress on either seems much too elusive.

Another challenge posed by increased chemical facility security pits the need for public information and awareness against the effort to keep facility plans and strategies out the hands of terrorists. Documents on emergency response plans and chemical plant preparedness have been removed from the Internet and other public sources. The question remains whether that loss of transparency enhances security more than it shields poor planning from needed public scrutiny.

As in other areas of terrorism preparedness, the chemical industry and those who regulate it are hard pressed to answer the question, "Prepared for what?" Without threat-based standards against which to measure security spending, money and time are being wasted lurching from crisis to crisis, as each Code Orange alert and sensational media incursion highlights new vulnerabilities.

The Department of Homeland Security is conducting an inventory of America's critical infrastructure and formulating preparedness standards to secure key industrial targets from terrorists. The Assistant Secretary of DHS for Infrastructure Protection, Mr. Robert Liscouski, will testify on the status of those efforts. We appreciate his being here.

State and local officials, industry association representatives and an expert from the U.S. General Accounting Office will also testify. We appreciate the time, dedication and expertise of all our witnesses and we look forward to their testimony.

Mr. SHAYS. At this time the Chair would recognize Michael Turner, the vice chairman of the committee.

Mr. TURNER. Thank you, Mr. Chairman, for being at this field hearing. You have been instrumental in leading this community's charge to improve our homeland security and to assist our first responders in being prepared for threats that our country now faces.

I would also like to thank Representative Tim Murphy for hosting us here today and bringing this important issue of chemical plant security before this subcommittee. Representative Murphy is a leading member of the Government Reform Committee and effective legislator and colleague, served as vice president of our freshman class, and has been a strong advocate in the areas of homeland security, education and health care.

The issue of security of chemicals facilities is very important to our Nation. I'm encouraged to see that the private sector has taken a lead in preparing security assessments of not only their facilities, but also for the process of moving chemicals from location to location.

However, the Federal Government should be a partner in that process and work with companies to develop quality, comprehensive risk management plans. I mentioned there are witnesses from the private sector today on how the Federal Government can be an effective partner in addressing these security concerns.

Since September 11 our knowledge of the threat we face of these facilities has changed, and so must our response. Under our chairman's direction, this subcommittee has reviewed issues from first-responder resources, our police and fire, nuclear power plant safety, our Federal nuclear weapons storage programs and the issue of the safety of our disposal of our Nation's nuclear weapons stockpile.

This issue today is important, of course, to our national security, but it is also important to our communities and our families who are in close proximity to these plants and could be affected by our preparedness. That is why it is so important that Congressman Murphy has requested that this field hearing be held here today rather than Washington, an area where the community and the families are affected most by this issue. Thank you.

Mr. SHAYS. Thank you, gentleman.

I recognize Mr. Murphy.

Mr. MURPHY. I thank you, Mr. Chairman, and I thank you for convening this hearing here in Moon Township, in Pittsburgh where we have many members of the chemical industry with plants, manufacturing and storage facilities.

We know that securing America's chemical facilities has long been a priority for the chemical industry and the thousands of people living in communities near large storage of potential hazardous materials. I'd like to thank not only Chairman Shays for coming here to this special field hearing, but also all the staff who has worked on this issue.

As you probably know, a local newspaper reporter, Carl Prine, and the TV media in this town have done a series of investigative reports on the very serious concerns about the levels of security we have at chemical facilities since the terrorist attacks on September 11, 2001; even CBS picked up the story, and 60 Minutes aired a show highlighting the impact of this issue across the United States.

In the last 2 weeks, the National Security Subcommittee staff has worked hard to make this hearing possible. I want to thank the witnesses who are going to testify before this committee today. This is a complicated issue of tremendous concern to countless citizens across the country. Ensuring the security of the Nation's chemicals demands the attention of several different parties with often-times competing industries. There are no easy answers, but I appreciate the willingness of these individuals to participate in an ongoing conversation.

Now, I have to admit, I am somewhat disappointed the companies themselves declined our invitations to testify this morning. While I'm looking forward to the testimony to be given by representatives of the chemical industry and expect it to be very informative, the firsthand testimony of the steps various companies in the Pittsburgh community have taken to improve security since September 11th would have been invaluable.

I do appreciate the companies' concerns for revealing security procedures in a public forum; however, this committee will still pursue a careful and thorough review of their policies and procedures in the interest of public safety.

I believe chemical facilities are, in fact, concerned with the security of their sites and the safety of the communities in which they reside. It is, and always has been in the best interest of the companies to be conscious of the possible threats the chemicals they produce and store pose to both their employees and the families living nearby.

In recent days, the crux of this issue has not been only one of facilities housing large quantities of dangerous materials should be required to conduct vulnerability assessments and then take action to reduce those vulnerabilities. The issue before us today is simply asking who should be responsible for regulating those assessments and improvements.

Federal, State and local governments have always played an integral role in ensuring that a certain level of security is maintained at chemical facilities, and had the companies testified today, we probably would have heard about all the different regulations they already are required to adhere to and the various government agencies that impose them.

Many of the facilities currently meet standards set by the Environmental Protection Agency, the Department of Transportation, the Coast Guard, State environmental agencies, State emergency management agencies and local municipalities.

Our immediate response should not be to automatically slap industry with additional security measures without first thoroughly investigating the issue; however, there are many hard questions that must be answered. Could more be done? Should more be done? And who should oversee it and at what cost?

Each of the witnesses that we hear today represent the different seats at the security table. I'm looking forward to hearing from witnesses at the Federal, State, local industry levels. Not only will we be hearing testimony from Federal industry representatives on the appropriate balance that should be struck in determining oversight and assessment authority, but we will also hear from a local township supervisor testifying to his firsthand experience working to in-

crease security at a local company. We will also hear from the chief of the Allegheny County Department of Emergency Services on the relationship that the department has with local businesses with large chemical stores and emergency response plans in place.

Finally, let me say this: Any decision made by Congress must be based on sound science and not initial knee-jerk reactions. The safety of the American people must be our top priority, and I firmly believe the best way to ensure their safety is to make the most informed and educated decisions possible. That is why this and future hearings on the issue are so important.

I thank you, Mr. Chairman.

Mr. SHAYS. I thank you, gentleman, and, again, appreciate this invitation to have this hearing here rather than in Washington.

To take care of some housekeeping first before calling on our witnesses, I ask unanimous consent of all members of the subcommittee be permitted to place an opening statement in the record and that the record remain open for 3 days for that purpose. And without objection, so ordered.

I ask for the unanimous consent that all witnesses be permitted to submit their written statements in the record. Without objection, so ordered.

At this time I'll recognize our three panelists, our three participants in our first panel, the Honorable Robert P. Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection, Department of Homeland Security; Chief Robert Full, chief, Allegheny County Department of Emergency Services; and Mr. Thomas W. Headley, vice chairman, Forward Township Board of Supervisors.

I think you all know that it's our custom on this committee to swear in our witnesses, and at this time we would just ask you if you would stand and raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. Note for the record our witnesses responded in the affirmative.

I've chaired this subcommittee and the previous subcommittee now for over 8 years, and we've sworn in every witness except one, and you probably could guess that it was I who essentially chickened out. But other than that, everyone has been sworn in, so thank you very much.

We're going to start with you, Mr. Liscouski, and then Chief Full and then Mr. Headley. We'll go in that order.

At this time I'm turning over the Chair to Mr. Murphy, so you're in charge.

Mr. MURPHY [presiding]. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you, Mr. Chairman.

Mr. MURPHY. Actually, before I do that, I should make sure I understand how much time each Member has.

Mr. SHAYS. We're going to give you 5 minutes. We're going to roll it over for another 5 minutes. So you have 10 minutes, but feel free to be somewhere in that range of 5 to 10, and that's how we'll proceed, and then I think what we can do is 10-minute questions for each Member that we ask.

Mr. MURPHY. Thank you. And, Mr. Liscouski, you can proceed.

STATEMENTS OF ROBERT P. LISCOUSKI, ASSISTANT SECRETARY OF HOMELAND SECURITY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; ROBERT FULL, CHIEF, ALLEGHENY COUNTY DEPARTMENT OF EMERGENCY SERVICES; AND THOMAS W. HEADLEY, VICE CHAIRMAN, FORWARD TOWNSHIP BOARD OF SUPERVISORS

Mr. LISCOUSKI. Thank you, sir. Thank you for the opportunity to appear, Mr. Chairman, and members of the committee. I am pleased to be here this morning before your subcommittee to discuss the Department's efforts to protect and secure our Nation's critical infrastructure.

The Department's Information Analysis and Infrastructure Protection Directorate carries out comprehensive assessments of the vulnerability of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States.

Our overall protection methodology leverages an integrated physical/cyber protection approach to reduce vulnerabilities and to optimize our response when an attack does occur. Because of the disproportionately high physical threat facing U.S. chemical facilities, however, my remarks for today's hearing are directed at our physical security efforts toward safeguarding U.S. chemical facilities.

The IAIP Directorate has a dedicated organization committed to protecting physical assets that includes the Infrastructure Protection Office for which I am responsible. The organization responsible for protection is the Protective Security Division. Today I am here to give you a progress report on where we are now and what we have in store for the coming months to implement the President's National Strategy for Homeland Security as it relates to chemical security.

Since last year the Office for Infrastructure Protection has implemented a consolidated and coordinated team of physical security professionals. These experts were charged with responsibility for the following: Identifying critical infrastructure and key assets; assessing their vulnerabilities; assessing the risk to and the consequences of an attack against those infrastructures and assets; and working with State, local, territorial and private sectors to implement appropriate security measures.

More specifically, the Office of Infrastructure Protection is working to improve the safety and security of the Nation's chemical plants and facilities as part of the infrastructure protection directives in the Homeland Security Act and the National Strategy for Homeland Security. Despite the many organizational and cultural challenges associated with integrating these elements into one entity, our initial efforts have yielded effective, tangible and measurable results.

Every day at DHS we ask ourselves how are we safer today, and how do we measure our progress? Today I have some answers to those questions. Since its inception in 2003, less than a year ago, DHS, and specifically my office, has placed chemical site security on the top priority list for physical infrastructure protection.

We have managed Operation Liberty Shield, a domestic protection strategy that includes the deployment of members of State and

local police officers, the National Guard to approximately 150 sites across the United States, over half of which are chemical sites.

We have conducted a national risk analysis of the chemical sector to identify the most hazardous and highest-risk sites. We have deployed DHS protective security counterterrorism specialists to top priority chemical sites to identify vulnerabilities to attacks and develop prevention strategies with site management and local officials, and we have completed vulnerability assessments, developed specific buffer zone security plans and provided training and assistance to implement those plans.

This approach includes full engagement with the protective security community at the State and the local levels to include the private sector, and this has already resulted in the increased safety and security of millions of Americans living near the highest-risk sites.

We have developed a report on chemical facility common vulnerabilities. We have developed templates for protection plans for areas adjacent to those chemical facilities and a report on potential indicators of terrorist activities related to chemical sites which have been shared with State and local authorities. These reports have been published and distributed throughout the country to law enforcement authorities and to each of the States' homeland security advisor.

In addition, we are developing and using a graded approach to the approximately 66,000 sites. This is based on EPA records in the United States and identifying the 4,012 sites that should have vulnerability assessments performed. We are reviewing the amount of toxic materials stored at those sites, developing plume modeling for 146 chemical plants using the National Atmospheric Release Advisory Center [NARAC], for more detailed effects prediction.

We're reviewing the population density in the vicinity of large amounts of toxic chemicals and evaluating possible impacts of intentional attack as opposed to accidental release models used in safety programs.

High-risk sites will be visited on a regular basis to assist in the implementation of security recommendations, and we will also visit additional sites to provide training, support and recommendations, and we will do further followup visits on a regular basis. These visits and the protection plans will reduce risk to millions of Americans.

The Office of Infrastructure Protection's close association with the industry is exemplified by our close interaction with more than 20 Information Sharing and Analysis Centers [ISACs]. One example of this interaction is the Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, which was published by the American Petroleum Institute and collaboratively crafted by my office and the API, published in May 2003.

Protecting our critical infrastructure is a Departmentwide responsibility. In 2002, the Maritime Transportation Security Act was passed. Regulations now in place require some 5,000 sites to provide security plans to the Coast Guard, including 289 chemical facilities which were included in that list. Security plans are being prepared and submitted as we speak.

The Environmental Protection Agency [EPA], is another agency we work closely with. Historically, the EPA has been charged with identifying chemical and other substances that could affect the quality of the air we breathe and the water that we drink. Part of their mission includes regulations requiring chemical facilities that meet or exceed certain guidelines to develop and update these documents that are called risk management plans. These plans center on accidental releases of chemicals harmful to humans into the air or the water. The EPA published that there are about 15,000 chemical plants in the United States.

Before detailing our future programs and initiatives, however, I would like to address the EPA numbers as they are being used by the media and others regarding security at chemical plants. While these facts may adequately address environmental, emergency preparedness, and first responders' concerns, they do not appropriately reflect the possible results of terrorist attacks. Our analysis of terrorist scenarios show that of the 15,000 or so chemical sites identified by the EPA, approximately 4,000 if attacked would affect populations of 1,000 or more.

Over the next year the DHS will engage with approximately 4,000 sites, chemical sites, throughout the United States to continue to enhance security of our critical infrastructure sites in the chemical sector. These additional visits and protection plans will reduce the risk to tens of millions of Americans in 50 States, the District of Columbia and the U.S. territories.

The Department is working to ensure that the security of our Nation's critical facilities and infrastructure is a focus of our efforts.

I appreciate the opportunity to testify before you today, and I would be pleased to answer any questions that you have at the appropriate time. Thank you.

Mr. MURPHY. Thank you.

[The prepared statement of Mr. Liscouski follows:]

Statement of Robert Liscouski
Assistant Secretary for Infrastructure Protection
Department of Homeland Security



Good morning Mr. Chairman and Members of the Committee. I am pleased to appear before your Subcommittee to discuss The Department of Homeland Security's (DHS) efforts to protect and secure our Nation's critical infrastructure.

The Department's Information Analysis and Infrastructure Protection Directorate (IAIP) was established by the Homeland Security Act to access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to identify and assess the nature and scope of terrorist threats to the homeland; detect and identify threats of terrorism against the United States; and understand such threats in light of actual and potential vulnerabilities of the homeland.

In addition, IAIP carries out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States. These terrorist acts could be manifest in many forms, including attacks against our critical infrastructure, key assets, and national icons. Both physical and cyber assets have vulnerabilities that may be exploited by our enemies. The highly interdependent nature of our infrastructure makes physical and cyber weaknesses impossible to separate -- and difficult to address separately.

Our overall protection methodology leverages an integrated physical/cyber protection approach to reduce vulnerabilities and to optimize our response when an attack does occur. Because of the disproportionately high physical threat facing US chemical facilities, however, my remarks for today's hearing are directed at our physical security efforts toward safeguarding U.S. chemical facilities.

The IAIP directorate has a dedicated organization committed to protecting physical assets and includes the Infrastructure Protection (IP) Office for which I am responsible. That organization is called the Protective Security Division (PSD). Today, I am here to give you a progress report on where we are now, and what we have in store for the coming months to implement the President's *National Strategy for Homeland Security* as it relates to chemical security.

Since last year, IP has implemented a consolidated and coordinated team of physical security professionals. These experts were integrated from portions of the FBI, Department of Commerce, and the Department of Energy.

Specifically, IP is charged with the responsibility of:

- identifying critical infrastructure and key assets;
- assessing their vulnerabilities;
- assessing the risk to and consequences of an attack against those infrastructures and assets; and

- working with state, local, territorial, and private sectors to implement appropriate security measures.

More specifically, IP is working to improve the safety and security of the nation's chemical plants and facilities as part of the critical infrastructure protection directives in the *Homeland Security Act* and *National Strategy for Homeland Security*. Despite the many organizational and cultural challenges associated with integrating these elements into one entity, our initial efforts have yielded effective, tangible, and measurable results.

Every day at DHS, we ask ourselves "how are we safer today, and how do we measure our progress?" Today, I have some answers to those questions. Since its inception in March, 2003, IP has:

- Placed chemical site security on the top priority list for physical infrastructure protection.
- Managed Operation Liberty Shield, a domestic protection strategy that included deployment of members of the National Guard and state police to approximately 150 sites across the United States, over half of which are chemical facilities.
- Conducted a national risk analysis of the chemical sector to identify the most hazardous and highest-risk sites.
- Deployed DHS protective security counterterrorism specialists to top priority chemical sites to identify vulnerabilities to attacks and develop prevention strategies with site management and local officials.
- Completed vulnerability assessments, developed specific buffer zone security plans and provided training and assistance to implement those plans.

By the end of this year, we will have built on these accomplishments by:

- Reducing vulnerabilities through implementation of physical and cyber protective measures at 1700 high risk chemical, nuclear, and soft target sites
- Increasing security at the 500 of the 1000 highest risk sites through deployment of protective security advisory teams to implement protective measures and train owners and operators in incident response and protective measure implementation

This approach includes full engagement with the protective security community at the state and local levels, and this has already resulted in the increased safety and security of millions of Americans living near the highest-risk sites.

We have developed:

- a report on chemical facility common vulnerabilities;
- a template for protection plans for areas adjacent to chemical facilities; and
- a report on potential indicators of terrorist activities related to chemical sites.

These reports have been published and distributed throughout the country to law enforcement authorities and to each state's Homeland Security Advisor.

Additional Actions Taken by IP

We are:

- developing and using a graded approach to the approximately 66,000 chemical sites (based on EPA records) in the U.S. and identifying 4012 sites that should have vulnerability assessments performed;
- reviewing the amount of toxic materials stored at those sites;
- developing plume modeling of 146 chemical plants using the National Atmospheric Release Advisory Center (NARAC) for more detailed effects prediction;
- reviewing the population density in the vicinity of large amounts of toxic chemicals; and
- evaluating possible impacts of intentional attack as opposed to the accidental release model used in safety programs.

High-risk sites will be visited on a regular basis to assist in implementation of security recommendations. We will also visit additional sites to provide training, support, and recommendations and will do regular follow-up visits. These visits and protection plans will reduce the risk to millions of Americans.

IP's close association with industry is exemplified by our close interaction with the more than 20 Information Sharing and Analysis Centers (ISACs). One example of this interaction is the *Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries* published by the American Petroleum Institute (API) that were collaboratively crafted by IP and API and were published in May of 2003. A more recent collaboration with the Chlorine Institute and the American Association of Railroads included a joint program to reduce vulnerabilities of rail cars used for chlorine transport.

Protecting our infrastructure is a Department-wide responsibility. In 2002, the Maritime Transportation Security Act was passed. Regulations now in place require some 5000 sites to provide security plans to the Coast Guard, 289 chemical facilities are included. Security plans are being prepared and submitted as we speak.

The Environmental Protection Agency (EPA) is another agency we work closely with. Historically, the EPA has been charged with identifying chemical and other substances that could affect the quality of the air we breathe and the water we drink. Part of their mission includes regulations requiring chemical facilities that meet or exceed certain guidelines to develop and update documents that are called Risk Management Plans (RMPs). These plans center on accidental releases of chemicals harmful to humans into the air or water. The EPA published that there are about 15,000 chemical plants in the U.S.

Before detailing our future programs and initiatives, I would like to address these EPA numbers as they are being used by the media and others regarding the security at chemical plants. While these facts may adequately address environmental, emergency preparedness, and first-responders' concerns, they do not appropriately reflect the possible results of terrorist attacks. The IP analysis of terrorist scenarios shows that of the 15,000 or so chemical sites identified by EPA, about 4000, if attacked, would affect populations of 1000 or more.

Conclusion

Over the next year, the DHS will engage with approximately 4,000 chemical sites throughout the United States to continue to enhance security of critical infrastructure sites in the chemical

sector. These additional visits and protection plans will reduce the risk to tens of millions of Americans in 50 states, the District of Columbia, and U.S. territories.

Working with industry, local law enforcement and state and local officials in close partnership, the Department is working to ensure the security of our nation's chemical facilities and infrastructure. I appreciate the opportunity to testify before you today. I would be pleased to answer any questions that you have at this time.

Mr. MURPHY. We will now turn to Chief Robert Full, who is the chief of the Allegheny County Department of Emergency Services. Chief, please proceed.

Chief FULL. Good morning, Mr. Murphy, Mr. Chairman, thank you very much, and members of the committee, I thank you for this opportunity to provide testimony before you today. Also, on behalf of Chief Executive Dan Onorato, our Allegheny County Chief Executive, I would also like to thank you for being here in our fine county as well, and rest assured your safety is paramount to us, and we wish your stay here to be very well.

I come before you not only as the Chief of the Department of Emergency Services, but also the Allegheny County emergency management coordinator, the chairman of the Allegheny County Local Emergency Planning Committee and also the Pennsylvania Region 13 Counterterrorism Task Force.

Mr. Murphy, I'd like to compliment you on your efforts and your interest in our things that we do here locally, as I know that you've attended our meetings before and provided us a great deal of support in our endeavors with not only terrorism, but also safety in the community.

Allegheny County, PA, has a population of 1.28 million persons in a 730-square-mile area, with 130 municipalities including the city of Pittsburgh. The county is a large center for research and development, retail, manufacturing, specialized medical care centers, major educational institutions and numerous other industries and small businesses.

The county is a major transportation hub for North and South, East and West travel nationally via U.S. interstate highways, Pennsylvania State highways as well as local roadways; home to the Pittsburgh International Airport, major railroads, underground and above-ground pipelines, traffic tunnels, downtown subway, hundreds of bridges, and the three rivers recognized as being the busiest inland water port in the United States.

Allegheny County has 235 chemical facilities which the EPA has classified as having at least one or more of the extremely hazardous substances on their list of 300 with an additional 700 others requiring EPA 312 reporting.

This hearing is actually being held less than 2 miles away from one of the focal chemical facilities on the 60 Minutes program. That particular facility lies here in Allegheny County in an area that sits upwind from the city of Pittsburgh. With prevailing weather conditions such as today, any major release, accidental or intentional, would drift into the downtown population center within 10 to 15 minutes; before then even tens of thousands of people would be affected.

We can all sleep at night through the efforts and success of local, State and Federal Government working together to craft key legislation such as the SARA Title III laws that occurred back in the 1980's, as well as here in Pennsylvania when the Pennsylvania Legislature enacted Pennsylvania Act 165. These two pieces of legislation and others are responsible for ensuring that plans, training and exercises, information, funding, accountability, emergency response and mitigation of programs are in place to ensure the safety of our community. Chemical safety has been taken very seriously

here, and we've been recognized as being much ahead of the curve in prevention and response to chemical releases either from fixed facilities or a transportation accident.

Security of our chemical facilities from an intentional act from within their own employees as learned from that tragic event in Bhopal, India, or an act of domestic or international terrorism has been an issue with our local emergency planners and local emergency planning for years, long before September 11th. I am and those particular groups, the LEPC, are in favor of legislation to ensure the security of all facilities that use, store and transport chemicals.

The facility that was the focus of the 60 Minutes program was one of our upstanding chemical facilities that sit on our LEPC and have one of the finest safety records that we have here, and we enjoy a great working relationship. We, too, at the local emergency planning committee and I personally was amazed to see the story and the issue in regards to access into their facility by the reporters.

The American Chemical Council has done an excellent job in being out front in the security issue, but I know firsthand that many of the companies that I am most concerned with are not members of the American Chemistry Council.

There continues to be facilities, many of them in my county here, that one could walk straight in under the guise of darkness and cause significant damage and public danger. Some of the facilities have no more security than maybe perhaps a padlock or a chain, and we would be lucky in those cases as well.

The first to respond to any emergency is always the affected local government followed by State and Federal Governments. The sharing of information on security issues pertaining to chemical plant security and transportation issues needs to be enhanced to include local law enforcement authorities and the local emergency planning committees as soon as possible.

Allegheny County, the Pennsylvania Region 13 terror threat assessments have all concluded that targeting one of our many chemical plants and/or the chemical transportation system ranks very high than the threat of something or somebody running through a neighborhood street discharging some sort of military war agent.

The best terrorist event to incur is never to let it happen in the first place, and this could also be said for fire safety as well. You can have the best trained and equipped fire department, but when the fire occurs, people get hurt, may die, and buildings are lost. All this can be minimized by good fire prevention, but not totally prevented. Strong fire codes and enforcement, smoke detectors, exit plans and sprinklers contribute greatly to reducing bad outcomes, so the best fire to have is not to have one in the first place.

We are continuing to improve our ability to respond to a WMD event locally and nationwide. Congress and the President and all of you have made available billions of dollars for homeland security at the local level, and it is finally beginning to be seen at the lowest levels of government and public safety in this county. This is for planning, training, exercises and equipping responders. I personally don't want to ever test that system.

Chemical security enhancement with the partnership of government as demonstrated with the great successes through SARA Title III as well as our local ordinances and our State laws through reasonable legislation and cooperation is a must. We need to do everything to ensure we never experience a terror attack again. We already know that chemical facilities and their transportation are a risk. Shame on us if we do not do everything possible to protect them. They sit in our counties, our cities, and towns and our neighborhoods.

Thank you very much.

Mr. MURPHY. Thank you, Chief Full.

[The prepared statement of Chief Full follows:]



Congress of the United States
House of Representatives
House Subcommittee on National Security, Emerging Threats, and International
Relations

Testimony Outline – Chief Robert A. Full
February 23, 2004

Chief Robert A. Full
Department of Emergency Services
Allegheny County, Pennsylvania

Emergency Management Coordinator: Allegheny County, PA
Chairman: Allegheny County Local Emergency Planning Committee
Chairman: PA Region 13 Counter Terrorism Task Force

Allegheny County, Pennsylvania has a population of 1.28 million persons in 730 square miles with 130 Municipalities including the City of Pittsburgh. The County is a large center for Research and Development, Retail, Manufacturing, Specialized Medical Care Centers, Major Education Institutions, and numerous other Industries and small businesses. The County is a major transportation hub for North / South, and East / West travel nationally via U.S. Interstate, PA State, and Local Roads. Home to Pittsburgh International Airport, major railroads, under ground and above ground pipelines, traffic tunnels, downtown subway, hundreds of bridges, and the Three Rivers and recognized as being of the busiest inland water ports in the United States. Allegheny County has 235 Chemical facilities classified by the EPA as storing and/or using one of their 300+ chemicals as identified as Extremely Hazardous Substances requiring EPA 302 reporting, and 700 others requiring EPA 312.

Mr. Chairman and Members of the Committee thank you for the opportunity to comment.

This hearing is being held within 2 miles of the heaviest concentration of chemical use, storage, and transportation in this County. That area sits upwind from downtown City of Pittsburgh. With prevailing weather conditions any major release accidental or intentional would drift into the downtown population center within 10 to 15 minutes. Before then 10's of thousands would be affected.

We can all sleep at night through the efforts and success of Local, State, and Federal Government working together to craft key legislation such SARA Title III, and in Pennsylvania Act 165. These to pieces of legislation are responsible for ensuring that plans, training and exercises, information, funding, accountability, emergency response, and mitigation programs are in place to ensure the safety of our community. Chemical safety has been taken very seriously here, and we have been recognized as being very

much ahead of the curve in prevention, preparation, and response to a chemical release either from a fixed facility or a transportation accident.

Security of our chemical facilities from an intentional act from within their own employees as learned from the Bhopal, India event, or an act of domestic or international terrorism has been at issue with local emergency planners the Local Emergency Planning Committee (L.E.P.C.) for years long before September 11, 2001. I am in favor of legislation to ensure the security of all facilities that use, store, and transport chemicals.

The American Chemistry Council has done an excellent job in being out front on the security issue. I know first hand that many of the companies that I am most concerned with are not members of the A.C.C. There continues to be facilities in my County that one could walk straight in under darkness and cause significant damage and public danger.

The first to respond to an emergency is always the affected Local government followed by the State and Federal Governments. The sharing of information on security issues pertaining to chemical plant security and transportation issues needs to be enhanced to include local law enforcement authorities, and the Local Emergency Planning Committees.

Allegheny County and PA Region 13 terror threat assessments have all concluded that targeting one of our many chemical plants and/or the chemical transportation system ranks higher than the threat of someone running down a neighborhood street discharging some sort of military war agent.

The best terrorist event to incur is "never let it happen, in the first place" this could also be said for fire safety as well. You can have the best trained and equipped Fire Department, but when a fire occurs people get hurt, may die, and buildings are lost" All this can be minimized by good fire prevention, but not totally prevented. Strong Fire Codes and enforcement, smoke detectors, exit plans, and sprinklers contribute greatly to reducing bad outcomes. So the best fire to have is "not to have one, in the first place".

We are continuing to improve our ability to respond to a WMD event locally and nationwide. Congress and the President I you all have made available billions of dollars for homeland security at the local level and it is finally beginning to be seen down at the lowest levels of government and public safety in my County. This is for planning, training, exercises, and equipping responders etc. I personally don't ever want to test the system.

Chemical security enhancement with a partnership between Government and private sector through reasonable legislation and cooperation is a must. We need to do everything to ensure we never experience another terror attack. We already know that chemical facilities and there transportation are a risk. Shame on us if we do not do everything possible to protect them. They sit in our Counties, Cities, Towns, and Neighborhoods.

Mr. MURPHY. We will now hear from Mr. Headley, who is vice chairman of the Forward Township Board of Supervisors.

Mr. Headley, please proceed.

Mr. HEADLEY. OK. Before we start here, I'd like to make one correction to my written statement. The facility in question is now known as Univar, but was previously known as Vopak, and in my statement I've used both names, and the correct current name is Univar.

Thank you for the opportunity to address the panel this morning on an issue of local and national importance. My name is Tom Headley, and I'm vice chairman of the Forward Township Board of Supervisors, one of three part-time elected officials who form the governing body of our municipality.

Forward Township has a population of just less than 3,800 people in an area of more than 20 square miles. The area is mostly rural with a concentration of population around the town of Elizabeth and several small communities along the Monongahela River including the community of Bunola.

I am here today because Univar, a distributor which receives, warehouses and ships a wide variety of chemicals, has a large facility located in Forward Township at Bunola. This location is one of an estimated 123 chemical facilities nationwide with an accidental toxic release worst-case scenario where more than 1 million people in the surrounding area could be at risk of exposure to a cloud of toxic gas. Prior to September 11 people in the area were aware of this facility, and the various chemicals were present, but were not overly concerned. After that date, with increased potential for acts of terror against a facility of this type, the vulnerability and security of this plant became a major concern.

A meeting to discuss these issues with company management was requested. At this meeting our police chief, our emergency management coordinator and myself met with Vopak executives to review site security. It was apparent that a major upgrade was necessary. Our chief performed a site survey and developed a list of minimum security upgrades which the municipality would require. Management raised the issue of cost and indicated this expense would place them at a competitive disadvantage relative to others in their industry. I made it clear these improvements would be made either on a voluntary basis, or the township would pass ordinances mandating their completion.

I am pleased to report Vopak made the recommended improvements costing more than \$200,000. Perimeter fencing, automatic gates, security cameras and monitoring devices, improved lighting and security during off-hours were included. In addition, an emergency plan for the community was developed, a warning siren installed, and emergency information was distributed to all residents in the immediate area and downwind of the plant.

In spite of these changes, this plant remains vulnerable. The 30-acre plant site runs from a State highway, Bunola River Road, to the Monongahela River, and includes six buildings. The main line of the CSX Railroad bisects the property, and buildings are located on both sides. Each side is fenced; however, the main track and the siding where loaded tank cars of chlorine are stored is not secured. The quantities of chlorine present are the reason for the serious

worst-case scenario. In addition, there's a barge unloading facility located along the riverfront where chemicals are pumped from barges into storage tanks. More than 50 loads of various chemicals are shipped in and out of this location during an average day.

Should there be any type of security problem at the plant or with a load in transit while in the township, the Forward Police Department would be notified to respond. We have a professional department with five full-time and two part-time officers. Normally one officer is on duty per shift. Response time to an incident at the plant will depend on the location of the officer in the township and could be more than 10 minutes from the time the call was received.

Our officer can request and receive assistance from surrounding departments and Allegheny County, but, again, time is required for help to arrive. Our municipal budget is just over \$800,000 per year, and well over half that amount represents police department and associated costs. The township is not in a position to employ sufficient police to provide adequate security to meet the potential threats faced by this facility.

After reading the GAO report, GAO-03-439, I would like to make the following comments as a public official in a host municipality for a chemical facility, and I'll just hit the major points here. Those of you who have the written statement can see the specifics which I've added.

Security for chemical plants must be improved. The government must mandate reasonable minimum security standards at all locations which produce, process, warehouse or distribute chemicals and other hazardous materials.

Voluntary compliance or self-regulation by the industry is not appropriate in this situation. Substitutes for the most dangerous chemicals should be encouraged and strict limits placed on maximum allowable quantities of these materials at each location.

One agency of the Federal Government must be given specific overall authority for chemical industry security. My suggestion would be the Department of Homeland Security. The present shared security responsibility is unwise and unable to deal with today's potential threats.

The scope of any risk management plan must include not only the plant site, but also the risks inherent in the movement of materials to and from the plant.

Money for staffing, training and equipment for local police departments must be made available immediately, and any new risk management plan must think outside the box and anticipate non-traditional threats.

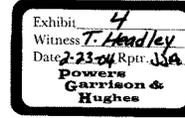
I thank you for your attention to this information. Security in these times is an issue which affects everyone regardless of location. From a huge city like New York with a population of many millions to the small town of Bunola with fewer than 300 residents, everyone is concerned about threats to their safety and well-being. Steps need to be quickly taken to minimize these risks, and the Federal Government must assume the lead role in this endeavor.

I will be pleased to answer any questions you might have. Thank you.

Mr. MURPHY. Thank you, Mr. Headley.

[The prepared statement of Mr. Headley follows:]

**Statement for Committee on Government Reform
Hearing Date: February 23, 2004
Presented by Thomas W. Headley
Vice-chairman-Forward Township Board of Supervisors**



Thank you for the opportunity to address the panel this morning on an issue of local and national importance. My name is Tom Headley and I am Vice-chairman of the Forward Township Board of Supervisors, one of three, part-time, elected officials who form the governing body of our municipality. Forward township has a population of just less than 3800 people in an area of more than twenty square miles. The area is mostly rural with a concentration of population around the town of Elizabeth and several small communities along the Monongahela River including the community of Bunola.

I am here today because Univar, a distributor which receives, warehouses, and ships a wide variety of chemicals has a large facility located in Forward Township at Bunola. This location is one of an estimated 123 chemical facilities nationwide with an accidental toxic release "worst-case" scenario where more than one million people in the surrounding area could be at risk of exposure to a cloud of toxic gas. Prior to 9/11, people in the area were aware of this facility, and that various chemicals were present, but were not overly concerned.

After that date, with increased potential for acts of terror against a facility of this type, the vulnerability and security of this plant became a major concern. A meeting to discuss these issues with company management was requested. At this meeting our police chief, Emergency Management Coordinator, and myself met with Vopak executives to review site security. It was apparent a major upgrade was necessary. Our chief performed a site survey and developed a list of minimum security upgrades which the municipality would require. Management raised the issue of cost, and indicated this expense would place them at a competitive disadvantage relative to others in their industry. I made it clear these improvements would be made either on a voluntary basis, or the township would pass ordinances mandating their completion.

I am pleased to report Vopak made the recommended improvements, costing more than \$200,000. Perimeter fencing, automatic gates, security cameras and monitoring devices, improved lighting, and security during off- hours were included. In addition, an emergency plan for the community was developed, a warning siren installed, and emergency information was distributed to all residents in the immediate area and downwind of the plant.

In spite of these changes this plant remains vulnerable. The 30 acre plant site runs from a state highway, Bunola River Road, to the Monongahela River and includes 6 buildings. The main line of the CSX railroad bisects the property, buildings are located on both sides. Each side is fenced, however, the main track and the siding where loaded tank cars of chlorine are stored is not secured. The quantities of chlorine present are the reason for

the serious “worst-case” scenario. In addition, there is a barge unloading facility located along the riverfront where chemicals are pumped from barges into storage tanks. More than 50 loads of various chemicals are shipped in and out of this location during an average day.

Should there be any type of security problem at the plant, or with a load in transit while in the township, the Forward police department would be notified and respond. We have a professional department with 5 full-time and 2 part-time officers. Normally one officer is on duty per shift. Response time to an incident at the plant will depend on the location of the officer in the township, and could be more than ten minutes from the time the call is received. Our officer can request and receive assistance from surrounding departments and Allegheny County, but again, time is required for help to arrive. Our municipal budget is just over \$800,000 per year, well over half that amount represents the police department and associated costs. The township is not in a position to employ sufficient police to provide adequate security to meet potential threats faced by this facility.

After reading the GAO report (GAO-03-439) I would like to make the following comments as a public official in a host municipality for a chemical facility.

Security for chemical plants must be improved. The government must mandate reasonable, minimum security standards at all locations which produce, process, warehouse, or distribute chemicals and other hazardous materials. Voluntary compliance or self-regulation by the industry is not appropriate in this situation.

- All plants containing hazardous materials regardless of size must comply
- Plants with larger quantities or extremely hazardous materials attractive to potential terrorists must meet much higher standards.
 - “Worst-case” scenarios must consider multiple, simultaneous uncontrolled releases of various hazardous materials as might be experienced in a terrorist attack. This is not the case with the present “Risk Management Plan” which is concerned with an “accidental” release from only one storage vessel when multiple vessels (railcars) may actually be present.
- Each plant must establish, and maintain, at their expense, a security force to deal with the potential threat presented by their facility. This cost cannot be borne by the host municipality. The federal government pays for baggage inspection and security at airports to deal with that potential threat, they might also assist with this cost. This security could be a private force under contract to the company, or a direct subsidy to a municipal police department to defray all costs for the required additional police protection.
- Once security upgrades are in place, security threat response training including company security, local and county police, and disaster response teams should be mandated on a regular basis. This joint training is presently being done for fire

and accidental releases but there is nothing, to my knowledge, dealing with security threats.

- These drills must anticipate an attack with the intent to blow up materials stored on site, as well as a one where materials are removed and taken to an off-site location. Truck diversions or hijacking scenarios must be included.
- Uniform federal regulations will “level the playing field” for each company and every location in the industry. All companies will face similar costs to meet the standards, none will be at a competitive disadvantage.

Substitutes for the most dangerous chemicals should be encouraged, and strict limits placed on maximum allowable quantities of these materials at each location.

- Liquid chlorine is required for treatment of drinking water and sewage among a multitude of other uses. Appropriate security costs for liquid chlorine should be included in the selling price. This would encourage use of more stable forms of this chemical and make safer substitute materials financially attractive to consumers.

One agency of the Federal Government must be given specific, overall authority for chemical industry security. My suggestion would be the Department of Homeland Security. The present shared security responsibility is unwise and unable to deal with today’s potential threats

- Listed below are just some agencies now responsible for regulating various phases of the operation of Vopak and this is not a comprehensive list.
 - Truck Transport in/out—Local police, state police, ICC, PA DEP, EPA, US Dept. of Transportation
 - Rail Transport in/out—Federal Dept. of Transportation, PA DEP, EPA
 - Barge Transportation in/out—US Coast Guard, PA DEP, EPA,
 - Plant Site—PA DEP, EPA, Federal DOT (Rail Lines & Spur)

The ability of these agencies to jointly develop and enforce an effective program is questionable.

The scope of any Risk Management Plan must include not only the plant site, but also the risks inherent in the movement of materials to/from the plant.

- Tank cars, box cars, tank trucks, regular trucks, and barges present attractive targets while en route to the plant especially in populated areas.
- The current identification system for chemical shipments should be reviewed. For example, chlorine cars, trucks, and containers are clearly marked chlorine. Does this make sense from a security standpoint?
- Examine the condition and maintenance, especially winter snow removal, of the

main travel routes used by trucks accessing the plant location.

Money for staffing, training, and equipment for local police departments must be made available immediately.

- Our police, the first responders to any situation at Vopak, have received chemical protection breathing equipment, but have not yet received chemical protection suits or boots. Should there be a security problem with a chemical release, our officer could only go to the perimeter of the plant property, assess the situation and request county assistance.

Any new Risk Management Plan must “think outside the box” and anticipate non-traditional threats.

- The possibility of crashing a small plane into a chemical plant or railroad tankers parked on a siding at a plant or in a rail yard.
- The possibility of an intentional or unintentional derailment near a siding containing hazardous materials.
 - At Vopak, chlorine tank cars are located on a siding next to the main line of the CSX. In spite of two nearby derailments over the past two years, we have been unable to require a low speed limit in the plant area. CSX management advises speed is the “discretion” of the locomotive engineer, and the authority to mandate a speed limit rests with a federal agency.
- The possibility of rail/truck collision at an in-plant or nearby rail crossing.
 - Again, Vopak was told the locomotive engineer is not required to sound the horn at “private” (in-plant)” railroad crossings or driveways.
- Investigate adequacy of container design (rail & truck tankers, smaller packaging) used for transportation of chemicals in light of current security threats. Most were designed to withstand “transportation accidents” not today’s security threats.

I thank you for your attention to this information. Security in these times is an issue which affects everyone regardless of location. From a huge city like New York with a population of many millions, to the small town of Bunola with fewer than 300 residents, everyone is concerned about threats to their safety and well being. Steps need to be quickly taken to minimize these risks and the Federal Government must assume the lead role in this endeavor.

I will be pleased to answer any questions you might have.

Mr. MURPHY. I'd like to start off by asking a couple questions of each of you. I think each Member has 10 minutes to ask questions.

Mr. LISCOSKI, let me first start off, if you could give us a general idea, what do you perceive is the greatest threat that chemical facilities face in a terrorist attack?

Mr. LISCOSKI. Sir, there's probably a couple of ways to answer that question. In the context of the different types of methodology that various terrorist groups will use to target facilities, they're always going to look at greatest consequence of loss depending upon the perspective of the group. So if I interpret your question to say which group is most interested in chemical facilities or types of attack—

Mr. MURPHY. Actually, groups and, yes, types of facilities.

Mr. LISCOSKI. I mean, we know al Qaeda has expressed interest in the past, based upon bogus reporting, to attack chemical facilities. We've had no specific reporting about those types of threats with locations, but we know generally speaking that's always been an area of interest.

We know, based upon their tactics in the past historically that they've not targeted specific chemical facilities overseas, but we know based upon how they conducted attacks in the past, we extrapolate from those tactics into what we think we need to protect against here.

Without going into great detail of those tactics, you know, we look at ways that they've attacked facilities in the past; we just extrapolate to those methodologies here in the United States.

Mr. MURPHY. One of the things that Mr. Headley has pointed out, that Forward Township has voluntarily complied and invested a great deal of money in some safety features. As I've read, one of the factors of the plant there and at other chemical plants that they can't control is they put fences everywhere else, but they cannot block rail traffic that actually goes to their facilities.

Is that my understanding, this rail traffic goes right by the—

Mr. HEADLEY. It bisects the property. It goes right through the middle. Both sides are fenced, but the center portion and the rail sidings is not fenced.

Mr. MURPHY. So someone could enter from there, or you could have a chemical or a train car go through there, too.

Are we doing some things to deal with assessing those vulnerabilities in the chemical plants and making changes there?

Mr. LISCOSKI. Mr. Chairman, we're taking a whole list of security concerns across the Nation, and we can talk about specific concerns and specific sites, but I'd like to start off with sort of the methodology and how we look at the prioritization of where we need to be putting our efforts.

And I'd like to open up again by stressing in terms of priority, we share very common concerns with the committee and with our State and local counterparts about the need to protect the Nation, particularly from the most dangerous threats that we face and where those consequences might manifest themselves, and my concern is in the chemical industry specifically. We know that we have a lot of work to do there.

Again, DHS will be celebrating our first anniversary here next week, and in the context of that, the focus we've had from day 1

when we opened the door has been on improving our chemical site security plans, our strategies, and, most importantly, putting tactics where we need to ensure that we can reduce the greatest vulnerabilities we have.

By way of context, there are many vulnerabilities across the United States in many critical areas, in many critical infrastructure areas, and even if we focus every single one of our resources on improving the chemical sector alone, we still couldn't do enough in 1 year to satisfy me. But clearly in terms of reducing the vulnerabilities, this is going to be a work in progress over a period of time. So we're prioritizing our efforts and looking at every available resource and tool we have in our tool kit to reduce those vulnerabilities.

So in the context of the respective vulnerabilities, job one we have is assessing those vulnerabilities to ensure that we understand what do we have to focus on first, and it's everything from chemicals being stored—if we focus on the chemical sectors for purposes of this hearing, looking at chemicals in storage, looking at chemicals in transit, identifying those vulnerabilities, the mitigation techniques necessary, what's effective and sustainable over time.

And to that end it's important to note here that a lot of the industry's concerns when they talk about money—and I'm not here representing the industry for a moment. I'll just tell you that from a practical perspective, sometimes any amount of money isn't sufficient enough to reduce the vulnerability in some cases without a long-term strategy about how that money is going to be implemented to reduce vulnerabilities over a long period of time.

So we look at tactics in terms of which we have—what tactics do we have to apply to reduce vulnerabilities in the immediate sense, those highest priorities. We look at strategies and tactics that we employ over time to develop cost-effective, sustainable and very effective programs that reduce the threat, and we can respond to threats in a very dynamic environment.

So to talk about which specific modality of theft in the context of chemicals in place or those chemicals in transit, we are looking at the entire chain of the chemical sector's vulnerabilities.

One other point and I'll conclude, and that is it's important to note that when we talk about the chemical sector and all sectors within the critical infrastructure, that we're not looking at things in the context of their single vulnerability or their single place in the critical infrastructure chain. With all these sectors there are interdependencies, and when we talk about the impact of the chemical sector and what we might be able to do to reduce very specific vulnerabilities, we may be creating other vulnerabilities by reducing those.

So we've got to take a very holistic look at the entire dependency chain around the companies' dependencies between the chemical sector, board of treatment, the production of pharmaceuticals and the impact of that, and this is something we look at very carefully, and there is a significant amount of work being done there as well.

Mr. MURPHY. Thank you.

Chief Full, let me turn toward you and ask you as someone who deals with local first responders, and obviously they would be part

of what we're dealing with here, I want you to describe for the board a scenario that there was some intentional attack on a chemical facility, what that would do to the region. And certainly there are areas of the Nation where the outcome of the worst-case scenario are looking at in the millions; though tragic here, it would be tens of thousands or hundreds of thousands or so. But the key in response to the first responders and medical facilities, do you conduct training with the chemical industry and fire and police departments and hospital personnel to cover various scenarios and drills of how one might react in this situation?

Chief FULL. Congressman, we do. We have, again, an aggressive, again, consequence management program here in Allegheny County which primarily does focus an awful lot on training and preparation and response with 5 Pennsylvania State-certified hazardous materials response teams, our 26 hospitals.

As you know, with our 130 municipalities, we have 217 separate fire departments, 119 police departments and 70 EMS agencies in our county alone, and we have worked hard over the many years here to bring their level of training up to at least hazardous materials awareness and recognition, and many more of the departments have been operationally trained.

There still needs to be a lot of work to be done. There again, through the processes of planning for a chemical facility release or a transportation accident in our county here, there's a different nature of the beast whenever you have responders that they're able to go out and respond to some sort of an accident or something that was unintentional. But there's a new dynamic now for first responders that are charged now with possibly responding to events that have been intentionally created with the full intent not only to kill and maim a number of the public, but also to kill them, even through the aspect of secondary issues, a secondary problem be established just to take out the first responders.

But we do do the training, and it has been funded primarily through the SARA Title III and local emergency management and planning committee funds that we secure from the chemical plants themselves. I believe we do have a strong partnership with those chemical plants, but at the same time we have not addressed and we have no knowledge really of the things that have been going on behind the scenes with security with them as well.

Mr. MURPHY. Let me ask you, too: The EPA is supposed to have on file, reports of the response management plan that you have for chemical companies, and that information is not being made public, but it should be accessible.

Have you been able to access that information?

Chief FULL. Yes, we have. And those reports are made available; the R&P reports and the Tier 2 reporting and all that reporting is made available to our office, and we disseminate that out to the local communities here in Allegheny County. It is also made available to the local fire departments as required under the law.

Mr. MURPHY. And has there been—we only have 2 seconds left for yourself and Mr. Headley—full cooperation and direct face-to-face conversations with the chemical companies to engage the information you need, training for those firefighters, etc., for those specific chemicals onsite.

Chief FULL. We have met with a very positive response in most cases in that regard. I'll tell you, Congressman, one of the things that concerns us the most is most of the folks are under the regulations, the current regulations. They're not our biggest problems and our biggest offenders, and many of the other offenders are the smaller businesses as well that we are concerned about that have things within their properties that fall just under the thresholds, but, you know, you can't make a determination. If you have a threshold planning limit of 1,000 pounds, can you tell me the difference between 999 pounds of that particular chemical and how it's going to react versus 1,000 pounds?

I would argue that there's not much difference, but there's many of the companies that have gone to—and what we want to do is we want to have them to limit their amount of storage and so forth. A lot of them have gone to putting their chemical storage in the transportation networks, and they have brought themselves a couple pounds underneath the reportable limits so they won't have to do additional planning, and they won't have to pay additional fees to reinforce and support our hazardous materials response program.

Mr. MURPHY. Mr. Headley, I'll give you a chance to respond to that, too.

Mr. HEADLEY. Well, I know that Forward Township, as I say, is home to one major chemical storage facility, and we have had orientations with the fire departments, not only our local fire department but the other likely fire departments who would come to assist. To my knowledge, the primary focus of that training was a fire situation or maybe an accidental release rather than an intentional problem caused by someone else.

And I'm not aware of all the training that's going on at the county level or the State level and the Federal level, but I would encourage a very strong emphasis on a coordinated response from the county because they're the ones that are best equipped to deal with a problem like this to get together with local police and emergency management people and train for a scenario where there is a willful act and an unintentional release as a result of that, and that would be my major suggestion.

Mr. MURPHY. I thank you.

I will now turn over to Mr. Turner, who, I should also note, as a former mayor of Dayton, OH, has particular insight of the eastern involved urban areas. Mr. Chairman.

Mr. TURNER. Thank you, Mr. Chairman.

I'm fascinated by all that has been accomplished without any particular legislative authority. If you listen to Mr. Headley and Chief Full and Mr. Liscouski, you talk about each of your agencies and communities and what you have done both with the private sectors and with companies, what the association for the Department of Homeland Security has done, there certainly are some impressive accomplishments.

So I think from your testimony we're hearing from each of you that there is a very wide gap in the ability to include everyone in this committee; but also in the sharing of information from successes, we know that we have some standards that we're all complying with.

Mr. Headley, you had cited the success that you had with Univar where you first approached the company and you requested access to the facility. And you were granted access to the facility where you were able to make recommendations, and through continued discussions with the company, they ultimately made changes, modifications as a result of your recommendations. And I wrote down one sentence from your testimony where you said: I made it clear these improvements would be made either on a voluntary basis, or the township would pass ordinances mandating their completion. Certainly after all this has come down to Congress as to our willingness to take action to provide the authority.

I want to go back to that very first meeting that you had with Univar when you requested access to the facility. Did you have any ability to compel or demand access if they had not invited you in?

Mr. HEADLEY. I really can't answer that question because that situation did not arise. These people have always been a good neighbor. They realized that they had a problem, we realized they had a problem, and we decided we would work together to solve that problem, and it was done on a very open and amicable basis.

My concern is there are probably—based on what I'm hearing from the other two gentlemen on this panel, there are numbers of other plants and facilities throughout the country who maybe don't have that cooperative attitude, and that's why my recommendation would be that you have to have some Federal legislation with some teeth in it to mandate that these people comply, because, being a businessman myself, everything comes down to cost, and you don't want to put one company at a competitive disadvantage to another, and if you do force some and not others, then the people who have not made the required improvements and made the required investments are going to be more competitive and will be able to sell at a lower price because they haven't spent the money. And that's not fair, and it doesn't make common sense.

Mr. TURNER. Your proactive efforts are certainly to be commended, and one thing that I thought of in hearing your description of doing an assessment and providing the company with information as to your recommendations is to what extent are we working to capture that.

Are you working with other agencies on a State or Federal level so that we can benefit from your experience so that when we look at the standards of other facilities, that might be able to be replicated?

Mr. HEADLEY. Well, most of the things that we did were common-sense things, and I think obviously somebody with a much higher degree of sophistication and ability, such as Department of Homeland Security and maybe the chemical industry, in concert should develop standards, because all we did, as I say, were common-sense things. I'm sure there are a multitude of other improvements and changes that should be made and could be made, but we are not aware of that.

Mr. TURNER. In your testimony in calling for Federal oversight and authority, you specifically identify the Department of Homeland Security as your recommended choice for that authority, and I wonder if you could give us your insight as to why you didn't choose the EPA where some individuals have advocated that.

Mr. HEADLEY. Well, in my printed statement I just—and this is not meant to be all-inclusive, but when you take a look at the entire problem, the storage and the transportation of chemicals, you have a multitude of various Federal agencies, and getting five or six different agencies or seven or eight different agencies to work together to do this is probably—it's probably not most effectively done on a cooperative basis.

My recommendation would be that somebody have the ultimate authority to require everyone else to go along, because there are too many people who have a piece of the regulatory or enforcement pie for any of them to do an effective job individually.

Mr. TURNER. Chief Full, in your testimony you also indicated that there was a need for Federal authority or for an agency to have oversight, but you did not identify a preference as to EPA or Department of Homeland Security. I wondered if you had one.

Chief FULL. I didn't do it intentionally. My recommendation would be the Department of Homeland Security.

I believe with all the efforts that have been done to date with channeling various levels of government into the Department as it would pertain to terrorism prevention and also security issues, even consequence management, I believe that has been very, very positive compared to the way it used to be with everybody having to go out and you would go on the Internet, or you would open up the White Pages, and you would go into that blue section and look what level of government, what agency covers this. But clearly I believe that this is something that the expertise lies in the Department of Homeland Security.

Mr. TURNER. Chief Full, have you experienced instances where there might be a company or facility where they have not been helpful in providing access? You don't have to name them, but I'd like you just to describe if that has happened and what your attempts might be to resolve that.

Chief FULL. Yes, we have. And literally we've been on the doorstep of chemical facilities that have had obvious leaks, even in progress, over the course of my experience and so forth where we had to stand there with law enforcement and threaten the arrest of the occupants of the building so we could gain access to see what was actually leaking in the chemical facility itself.

I come with 32 years of emergency response experience, and I've documented over 1,000 chemical spill responses in my career, and in my career in those chemical responses I've had the opportunity to experience a few of those situations. The vast majority of companies are compliant.

We probably have a greater threat—I know we're focused in on the facilities themselves. There's a lot of expertise that lies in the facilities, but I think that there is a tremendous void on the transportation networks and the quality of training of the drivers of the trucks that are carrying chemicals, and the railroads and the ready information that would be readily at hand.

If I had to pick my choice or the thing that would most disturb me or have the greatest consequence in our community would be an event regarding a chemical transportation incident. Obviously they would be moving the chemicals in and out of one of our facili-

ties, but there are great limitations in quick access to information and so forth in dealing with those from the first responder's aspect.

Here in our county, being a major transportation network, we fear even out here on the local interstate when a truck driver carrying some very serious chemicals—and they're all very serious, some of them are as serious as the Bhopal chemical that was released in Bhopal—that if the driver decides at a rest stop to go in and take a rest for a few minutes and leaves that truck running here, they can drive—pick up that truck and drive it into the downtown business district or through one of our communities.

We have the inland barge traffic here in our community here. Those barges carry 770,000 gallons of various chemicals. We have the second, I understand, largest chemical loading in our community of any inland port. All it would take is somebody with a—some sort of a small device to throw it off one of our bridges onto one of those tank barges, and we would have a significant problem.

A lot of other folks take a look at these extremely hazardous substances as well. We believe that the bulk storage chemicals, your fuels and even something as mundane as diesel fuel, can wreak havoc in a community.

We are known here as being one of the inland oil spill capitals of the world, and back in 1988 we had a significant release of over a million gallons of diesel fuel that went into our rivers that impacted our community for over a week with people not being able to draw water.

In 1987, we had a train derailment involving a major release of chemical and fire, which necessitated an evacuation of 16,000 people in the city of Pittsburgh for 2 days.

We know firsthand what it would take in the event that if we would have an act which would occur with these facilities in our neighborhoods and so forth, that we can't quickly enough protect the population, and there would be so many of them affected, and that's very hard to deal with.

Mr. TURNER. I thank you, sir.

I thank you, Mr. Chairman.

Mr. MURPHY. Thank you, Mr. Turner.

Mr. Shays.

Mr. SHAYS. Thank you, Mr. Murphy.

Following this panel we will have GAO address us, and I just would like to put in some perspective what we're going to hear and have all of you respond; Mr. Liscouski, you put into perspective the so-called worst-case scenario of 127—123 chemical facilities throughout the United States that could potentially expose 1 million people, 700 facilities that could potentially threaten 100,000 people, and 3,000 facilities that could potentially threaten 10,000 people. What does that mean?

Mr. LISCOUSKI. I think this is drawn from the R&P data base, sir.

Mr. SHAYS. Could you bring your microphone closer?

Mr. LISCOUSKI. Sure.

Mr. SHAYS. Thank you.

Mr. LISCOUSKI. I think the GAO data you're referring to is drawn off of the R&P data base by EPA.

Mr. SHAYS. What does that mean, though? I don't know how to translate it. I mean, I want to give you an opportunity to tell me what it means.

If you're saying there are 123 chemical sites that could negatively impact a million people, I need to know as a legislator what that means. I don't know what that means. I want to know what it means to you; I think I know what it means to me.

Mr. LISCOUSKI. First off, I think we have to level-set the numbers. The numbers that we're dealing with from that lineup to the R&P data base of 15,000 sites in that data base are drawn off of data based upon absolute worst-case safety-based scenarios. Those don't correspond to what we look at from a tourism perspective and realistic plume models that would ultimately have to be projected and then a determination made upon how large of a population. So the numbers we're dealing with are somewhat different than the numbers off of the R&P data base.

When we went through the prioritization of the chemical sites around the United States, we had to apply more realistic and more deterministic models to understand what the impact of a terrorist attack would be, and then subsequently what the effect would be on the population. So our numbers are different than what's been purported in the R&P data base to allow us to really focus on realities based upon the plume modeling. So we're drawing off of two sets of data, sir.

Mr. SHAYS. This committee began to undertake the terrorist threat in 1999. We rewrote our rules so that we would look at terrorists at home and abroad. We had 20 hearings before September 11th, in which we discussed various scenarios. We had the three primary commissions come before us: Hart-Rudman, Gilmore and the Bremer Commission. They all agreed there's a terrorist threat, they all agreed that we needed a new strategy, and they all agreed we needed to reorganize the government, but Hart-Rudman ultimately was the most radical.

When we and this committee talked to Americans before September 11th about the need to reorganize and create a Department of Homeland Security, the basic response was, what are we, Great Britain? There was just no willingness to come to grips with the terrorist threat. We had September 11th, we basically took the Hart-Rudman model, we created a department that you now work for.

Is it your sense that it was a wise thing in creating the Department of Homeland Security?

Mr. LISCOUSKI. Without question. I mean, without question, because I think the opportunities that have been presented to DHS for coordination for preparedness response, protection response without question have added value to America's security.

Mr. SHAYS. Well, we probably should have done it sooner, no doubt about that. The reason we didn't do it sooner in part was those in government didn't fully comprehend the threat, and clearly the public didn't.

And so I'd love to get a sense from you how much do you think the public has a right to know about the threat? I mean, in this community, for instance, what are they allowed to know, and where do we draw the line?

Mr. LISCOUSKI. If I can just take the liberty of engaging with you just to describe it further, because my sense when we say was there a right to know the threat, the public has a good understanding of the threat, we have a duty to inform the public about the threat, so we clearly communicate threat information fairly robustly and, in some folks' consternation, probably too much information at times. And we don't have perfect information, but that's just the nature of the intelligence that we have access to. But there are many other components to managing the threat, and I believe, sir, that's what you're referencing when you ask the public's right to know.

Mr. SHAYS. Not just the threat. I don't mean threat in a generic way, code orange and so on. I mean does the public have a right to know about vulnerabilities?

Mr. LISCOUSKI. Vulnerability, that's what I was about to get to. There's a whole chain of events that goes into protecting the public, some of which, as we discussed, should not be within the public's purview for knowledge related to protection responsibilities and protection methodologies.

Mr. SHAYS. Can you give me a hypothetical what they should never have a right to know?

Mr. LISCOUSKI. Well, I can just talk holistically about what the program is, and maybe I can add some more clarity to the approach, and I would be happy to get down to the details.

As we heard Chief Full describe and Mr. Headley describe about their abilities to understand what they need to know about the— at the local level, there is no question, and DHS is actively engaged in this process, and I speak of DHS and the Federal Government at large in sharing that information with those State and local authorities who have to prepare, have to respond to, have to understand what the first-responder requirements are. In the context of working with State and local authorities, we share information with the local police through the Homeland Security Advisory and through other mechanisms about protective methodologies and vulnerabilities.

So we regularly share with the public in the context of the authorities that ultimately have responsibility at the local level to interact with the public. The constituencies here are many and varied, and I wouldn't want to speak for either gentleman on each side of me about how they view their respective constituencies, but clearly we all strive to share as much information as we can, and I think we do a pretty good job at it, but clearly we need to do a better job at it, there's no doubt about that.

We have a number of information-sharing mechanisms to go out to the public, to the private sector, to the State and local governments. Since DHS has been established, the Information Sharing Analysis Centers, the information bulletins we regularly and routinely put out not just about the threat information to raise the alert level, but on preparedness and prevention and protective measures, which we routinely share with all government.

So I think we're in agreement, sir, about the public needing to know. We clearly share the information, so I appreciate your perspective.

Mr. SHAYS. OK. I'm not sure if we're connecting because I find tremendous reluctance on the part of the government to inform the public, and, for instance, I find it beyond my comprehension to know why—what code are we at right now?

Mr. LISCOUSKI. Yellow, sir.

Mr. SHAYS. Yellow means there's a likelihood for an attack.

Mr. LISCOUSKI. It's elevated risk, right.

Mr. SHAYS. Elevated, in other words, it's not general, but we're acting like it's general, and to the general public it's general; you know, we're under a threat, but we're on one level above. But yet we went to code orange, which meant, you know, there was a serious likelihood of attack. We knew we had concerns about planes, and we had concerns about dirty weapons in public places. We told the public that basically they should continue to do what they normally do.

So, I mean, I have a pretty big dispute that you and I will have to resolve with the Department on going to code orange and yet telling people do what you normally would do.

But let me just ask you in terms here, if we have 123 sites that could impact a million people, as you pointed out and I agree with, the plume isn't going to go in 360 degrees. If it did, it probably would not have the concentration to be as deadly, at least as to the distances, as you got into more distance. But you have two sites here; you have the Neville Chemical and Univar, which is in your area. Don't we have a sense that the plumes will more likely go in a certain direction? Don't we have historic data that would tell us that would be the case?

Mr. LISCOUSKI. Yes, sir, we do. In fact, that's how we were able to further refine the R&P list from 15,000 to the list that we have of about 4,012.

Mr. SHAYS. No. That's different; 15,000 are the number of chemical plants.

Mr. LISCOUSKI. Well, 15,000 are the R&P data base, which I believe were reflective of an impact of 1,000 people or more.

Mr. SHAYS. Yes. But, see, 1,000 people or more to me doesn't tell me anything. That implies there's 1,000. Those 1,000 could be 100,000. I mean, the 1,000 or more—you get my gist?

Mr. LISCOUSKI. No, sir, actually, I don't. The R&P data base considered the worst-case scenario from an EPA perspective.

Mr. SHAYS. 4,000 sites.

Mr. LISCOUSKI. No, sir, 15,000. The R&P data base, which was drawn by EPA, considered the worst-case scenario as related to the plume modeling perspective, which is virtually a 360-degree plume model—

Mr. SHAYS. Right.

Mr. LISCOUSKI [continuing]. Because of the safety concerns and what the EPA mandated from a safety perspective.

The plume modeling we applied from NARAC was a more realistic plume model based upon historical environmental conditions and the understanding of where the plume models would impact on the populations, and we adjusted that within the context of the plume model to, again, be a worst-case scenario, further refine the numbers.

Let me just respond to one thing you mentioned earlier.

Mr. SHAYS. I'm not quite sure—you can go on to your agenda, but I'm not quite sure you responded to what I'm just trying to understand.

Mr. LISCOUSKI. Sure. And I apologize. I'm not trying to obfuscate you, I'm trying to understand your question.

Mr. SHAYS. You have a lot of knowledge, and I want to make sure I know it, but allow me to understand. We're not talking about 4,000 sites; 1,000 more—

Mr. LISCOUSKI. Yes, sir, 4,000 sites.

Mr. SHAYS. Let's just deal with 4,000 sites, 1,000 or more. What I was trying to convey to you is when you—let me just tell you why I have this bias—

Mr. LISCOUSKI. Sure.

Mr. SHAYS [continuing]. And concern.

I voted for the Patriot Act. A majority of my constituents aren't sure they like the Patriot Act, I'm making that assumption. Congress repealed the power of us to go into a library, take the hard disk, understand who a terrorist may be talking to, being able to not have to tell the terrorist that we think they're a terrorist so that they go back and continue to communicate so that we can improve our intelligence.

I happen to believe strongly in the Patriot Act. I've come to the conclusion that the public doesn't believe the Patriot Act because they don't think there's a terrorist threat out there. And I have certainly come to the conclusion they don't think there's a terrorist threat because I think we haven't conveyed a terrorist threat because we don't want people to be needlessly concerned.

And so in the process of trying to not scare people, we are, in my judgment, endangering the public and weakening our ability to get information, because some of the powers that we need in order to get information may disappear because we may not renew the Patriot Act.

I'm just trying to put context to my question—I have this basic view that we need to tell people a threat, and then they get some power to deal with it, and then we both have a good sense of why that's happening.

When you say 4,000 sites, 1,000 or more, there are how many sites with 100,000 or more of that 4,000, and that's what concerns me.

Mr. LISCOUSKI. And as we've gone through the refinement process, sir, that's precisely how we've begun to prioritize our efforts. So I think we're very much in alignment and understand our priorities as you've just articulated them.

One thing, as Chairman Murphy understands well, that we don't want to create a situation with the public where we create panic around the situation by not providing information. And by the same token, sir, you're a psychologist, so, therefore, you've got a much deeper background in this than I, but I know from the concerns that we have in terms of getting the public to do the right thing and providing enough information, I agree with you, not enough information can create the same condition as too much information which might be shared irresponsibly.

DHS, as you pointed out, I think, has been fairly good, and our track record has been very good over the past several months and

has gotten better. Sharing information with State and local authorities and sharing information with our industry partners and sharing information with the public, we've tried to give as much context around the threat to allow people to plan, to allow people to understand what the threat means to them.

The one thing we don't control, frankly, is the information that the Intelligence Community can ultimately generate and acquire, and the information, you know, that can provide the appropriate level of context to the general population.

Mr. SHAYS. Let me just ask our two other participants—do you mind if I have an additional 5 minutes?

Mr. MURPHY. Not at all.

Mr. SHAYS. Have you both been told about plume modeling at either site, and do you have a sense of where these plumes go?

Chief FULL. I have not been told of those. I know in our own planning we do for accidental releases, we deal with the fact that we have prevailing weather issues, but we also have experienced events here that with that type of release that we've had instantaneous wind changes and things along those lines, and my experience lends itself to that even though that we know it's going to go probably in one direction, that through a course of a major event, it could go and turn around. And we have had past history in that regard. We have no knowledge of that. Usually when we're asked, it's emergency planners, plant people that have said, what do you think the worst case is? But there's very little or no science behind it.

Mr. SHAYS. Mr. Headley, are you pleased with the security model?

Mr. HEADLEY. Pleased is a relative term. We're certainly far better off than we were 2 years ago, but I think there's some room for improvement.

If I might want—I'd like to add one other thing, and in Mr. Liscouski's favor I think what we have here is EPA—information that was developed that the EPA modeled for one purpose, and we are trying to use it possibly for another purpose. And I think it's important that Homeland Security or whoever it is that's charged with the responsibility to do an accurate assessment given a terrorist scenario rather than an accidental release scenario, which is what was used to develop the EPA model.

And one thing, not to alarm anyone, but the EPA model is based, I believe—I'm not an expert on this—on the largest uncontrolled release from one particular vessel, whether it be a tank or a tank car or a truck or whatever; it did not anticipate the possibility for multiple releases from multiple trucks or tanks or railroad cars, and we have those scenarios in a terrorist situation that weren't present in an accidental release scenario, and I think those need to be examined.

Mr. SHAYS. Coincidentally, Mr. Murphy and I are participating in an exercise called Dark Porthole, which will address the potential impact of a combination of different types of attacks.

I feel like I'm just starting to edge into something that I would like to get into in more depth, but I guess what I'd like to ask all three of you is EPA is not here, and I have my own sense of why they're not here, they refused to come, and yet EPA has the exper-

tise, it seems to me, at least in the past, and they have—it seems to me that a terrorist attack would create a greater challenge than one that would be national—first of all, let me back up and say the chemical industry has an unbelievably good record of safety. It is just astounding in one sense how successful it has been, but that's based on everybody doing their job and people of goodwill working in the plant; it's not based on someone infiltrating the plant. It's not based on a plane attack, so on and so on.

So I guess what I'd like to ask as my last question for this round is should I believe that a terrorist attack would be less deadly or more deadly than what EPA has used as their scenario?

Maybe I'll start with you.

Mr. LISCOUSKI. Yeah, and I appreciate the opportunity to respond to that because I guess from my perspective as responsible for infrastructure protection, there isn't a single death that we want to live with. I think we have to level-set that.

We're getting kind of caught up in a numbers discussion here. We're going to be candid with you, it's not realistic to think we can prevent anything or every event. But I think our goal is to actually try to prevent every event that we possibly can.

Mr. SHAYS. See, the difference is that chemical plants we allow to be near the public because we thought people of goodwill would be in charge, and now the scenario is different. Just as before World War II, we moved chemical plants inland because we were concerned of their vulnerability on the shoreline. You know, that was World War II. Then we had a Communist threat, and now we have the terrorist threat, and the terrorist threat seems to me to change all the assumptions.

Mr. LISCOUSKI. Well, it does change all the assumptions, and the discussion we're having today is predicated on our thinking around the September 11 environment. And on that level we have to think about the DHS prospective and my colleagues here is that we have to think in a dynamic threat environment which does evolve.

So I think, you know, I'm glad to see the support for this because, quite candidly, the recognition of how challenging this problem is, is something which we need a lot of public education on. We are not standing still and remediating vulnerabilities in the highest priority sites that we have, and I wish I had a magic wand or a crystal ball—

Mr. SHAYS. My question I asked—and my time has run out—the question I asked was the EPA came out with their worst-case scenario, which we knew as a 360-degree plume and so on, but that notwithstanding, it seems to me, and correct me if I'm wrong, I can ask the next industry, but I'd like to know—I know what I'm going to ask them, and I don't know what they're going to say, but I want to know what you are going to say to the same question.

Do you believe that a terrorist attack in a chemical plant would be more serious, more likely to be more serious than one that would be accidental?

Mr. LISCOUSKI. Well, the potential is there. I mean, there's clearly no question when we talk about the potential, the potential for a terrorist attack to exceed an accidental release depending upon where we are on the scale, you know, that's just a reality.

Mr. SHAYS. So the question—

Mr. LISCOUSKI. I think in the various scenarios you have, I could come up with scenarios that would be less catastrophic than an accidental release. I can come up with scenarios that would be more catastrophic.

Mr. SHAYS. So what do you finally conclude?

Mr. LISCOUSKI. I'm concluding, sir, we're planning based on the priorities that we have of catastrophic loss. We're not stopping at a specific end line for total continuous improvement for the chemical sector.

I guess I don't want to be put into a box to say could a terrorist attack be worse than a worst-case scenario of an EPA release. I think if I look at the way the EPA data—

Mr. SHAYS. The answer would be yes.

Mr. LISCOUSKI. No, sir.

Mr. SHAYS. The answer would be yes.

Mr. LISCOUSKI. The answer would be no, then, I think, because the EPA worst-case scenario considers a 360-degree plume.

Mr. SHAYS. Well, other than the 360-degree plume.

Mr. LISCOUSKI. I can't qualify it.

Mr. SHAYS. You have to make assumptions.

Mr. LISCOUSKI. I am.

Mr. SHAYS. Let's just say the plume goes in one direction. I'm talking about the accident in a facility. Isn't it true that if you have an accident, you can focus on it; whereas, if it's terrorist, you might have more than one event in a chemical site and under that circumstance wouldn't it be worse?

Mr. LISCOUSKI. No, sir. I think there's a lot of education, I think, that has to go on here, and I regret that EPA isn't here. They could probably respond to their EPA modeling and what the worst-case scenarios are better than I because I don't pretend to be an EPA expert.

Mr. SHAYS. This is one of the things that this hearing has pointed out is that clearly the administration doesn't want EPA to be involved in this.

Mr. LISCOUSKI. I can't speak to why they're not here.

Mr. SHAYS. I am. I have the floor right now; I can speak to it. We've asked them—we know why they don't want to be here. We know there's a significant challenge. And one of the things before we let this panel go, I want to understand your relationship with the EPA.

I thank you for the time, and I'll come back.

Mr. MURPHY. Thank you, Mr. Shays.

I have a list of what EPA requires reports on, some 350 different chemicals that they're considered extremely hazardous substances of various levels.

As I look over this list, I mean, I obviously have to be a Ph.D. in chemistry to understand all the effects of all this, but, Chief Full, it brings to mind a comment you made earlier which particularly concerned me, and you said that companies may have some storage of some chemicals onsite, and that they may have to report or take certain actions if they are above a certain threshold, and they intentionally lower the amount of chemical onsite so that they do not have to take the same security steps. I want to make sure I understand that correctly. That's quite concerning to me.

Chief FULL. I don't believe that I can justify that they may do it for security purposes, but we do know that they do it on the process of minimizing their exposure to pay for chemical fees and so forth that have been allowed under the particular law.

And so, you know, if they're doing it for security purposes, then that certainly would be very, very tragic and just very disturbing to me. But I know for a fact, and it's been just a—it's been an ongoing effort over the last several years that the chemical industry has reduced the amount of chemicals that are typically stored on their facilities, and much more of those chemicals are being placed into the transportation network versus being stored at plants.

Mr. MURPHY. Thank you.

Another question I have relates to first responders, and I know Congress has appropriated a significant amount of money over the last several years to deal with this. I mean, with the Clinton administration there was 100 million put into the budget in fiscal year 2001, and the Bush I budget was \$360 million, and then \$750 for 2003, \$750 million for 2004 and continue on with that.

And I know looking at the kind of grants the local fire departments receive around my area, and my colleagues can attest to that, too, are they getting the right kind of equipment needed in areas where there might be chemical vulnerabilities?

Chief FULL. Congressman, right now I can say that the money is beginning to get to the right level, but, you know, the first appropriations took place several years ago. It's taken way too long to be able to get some of the moneys and the purchasing done to the local level. And what's occurred here, I know in my county I can say that we have now put equipment out in the law enforcement community, the fire service, the EMS community, and enhanced our hazardous materials teams, but we are just scratching the surface on their needs.

And what we have found now, that now that the money has down to the local levels, the vendors now are being inundated with the request for equipment, they can't fill the orders fast enough. So I believe the logjam here in even Pennsylvania has been corrected, but the vendors, again, can't fill the orders fast enough, but we're satisfied right now with the way that the money is coming. There is concerns the way that—whether or not that they will be shut off anytime sooner, and as well we would like more discretionary control over how some of the moneys are being spent in regards to how they can be used for exercises and some particular training.

Mr. MURPHY. Thank you.

Mr. Liscouski, I have a question for you. Without revealing things that were given to us in security briefings, repeatedly we hear patterns of terrorists that they go back and repeat their goals and their tactics until they achieve some results. And we've heard repeatedly comments from Bin Laden and from other terrorist networks that they're looking at something on the level of spectacular or massive in terms of casualties or injuries in the United States.

In a chemical area—and actually a big chemical attack we had was not done by external terrorists at all, it was actually done in the Oklahoma City bombing. It was done with fertilizer and using other chemical components there in a way that the chemicals can be controlled, and someone can use chemicals for a weapon.

It comes down to when dealing with terrorists, they're looking for something that also shows the vulnerabilities. I mean, that's the terrorists; they want to frighten people to hurt the economy, to shut down industries and to really harm many people whether it's personally, healthwise, politically or whatever that is.

Are we in an area of intentional access where someone may take chemicals, purchase them legally or whatever, and use them in some way as weapons of mass destruction? Are we also making some headway on any sort of regulatory efforts in controlling that aspect?

Mr. LISCOUSKI. Sir, I can't speak to the regulatory aspects of that, that's an EPA issue; however, working closely with the FBI and other partners in the law enforcement community, the FBI has very strong authority on following up reports of incidents that might include sabotage or forging of documents for obtaining those materials for eliciting purposes. That's not within my area of responsibility and expertise. I can add value to it, but I'm afraid I wouldn't do it justice with respect to the Federal Bureau in that regard.

We're concerned about it. We look at all those vulnerabilities. I haven't seen specific reporting or evidence that al Qaeda is using those tactics to apply chemicals. I have seen reporting historically of other U.S.-based groups, frankly, that you are particularly referring to as well of using that type of—

Mr. MURPHY. More domestic terrorists.

Mr. LISCOUSKI. More domestic terrorists.

We're looking at all aspects. I don't want to minimize that as a threat. We look at all aspects of that, but I have to then relate to my stronger partnership with the FBI, other Federal and State and local agencies that have to remain investigative in the law enforcement field.

Mr. MURPHY. Thank you.

Mr. Turner, 5 minutes.

Mr. TURNER. I would like to go back to an issue that Chairman Murphy raised in the initial questions; that is, the availability of public information not on the issue of terrorist threats, but through the EPA processes and where we've allowed information to be out in the public and that might aid someone that has a threat potential for a facility.

I want to tell you that I'm a big fan of the community participatory process that the EPA laws, regulations have permitted. They give both environmental groups and community groups an opportunity to bolster the responses of government by actively participating, and then that way they can have a stake on the effect or outcome being positive in the regulatory process of responses at these facilities.

But we've already recognized that those very same processes that enhance the community's local participation also provide information to bad actors to recognize the testimony that, for example, the information concerning these facilities can be taken off the Internet.

I'd like, if you will, for each of you to talk for a moment about your concerns you might have about the availability of some of this information to the public and also then your concerns, and specifi-

cally Mr. Headley and Chief Full, of your desire—obviously the communities benefit from some of this information being public so the community can participate, but at the same time our terrorist threat has—might change our evaluation of that. I'd like you to comment.

First, Mr. Headley.

Mr. HEADLEY. Well, Chief Full is the one who could most adequately describe what the progression of information is from Homeland Security through our police department; and then whether that information is disseminated directly to the chemical industry and then through their chain, I really don't know.

I know that from time to time information is passed along, I believe, from the FBI to the police department that there is some concern about something specific, and our police department takes additional steps to try to recognize that threat. Beyond that I'm not—I don't have expertise to speak to that issue.

Mr. TURNER. Just to reiterate, the question is about—and I appreciate your comments, Mr. Headley, about terrorist threats, but my question is about the availability of information with respect to the regulatory process pertaining to planning for emergency responses, permitting processes for these facilities. So much of our information, including what is stored at a facility, how the facility might respond and what its vulnerabilities might be have been made public through the EPA process of allowing communities to understand what's going on in their backyard. I was just wondering about contrasting that with given the fact that this information is made available to the public, but it's also available to people who we would not want to have it.

Chief FULL. I wish I could give you a solid answer, Congressman. I have mixed emotions about it. I was one who was—very much like yourself, I was very supportive of being in the public arena.

We pride ourselves even with our local emergency planning committee here with 60 members, with a vast array of public and private participation and all the various groups and so forth, but since September 11th it's very hard to take out of the mind-set that somebody could realize that one of the products inside one of those facilities would be ideal to wreak havoc.

With that said, though, I believe that here at the local level there are ways to get around that, that government, as long as we've established a procedure that when people want information, and rightfully so—I mean, a resident living next door to a community chemical plant should still have the right to be able to see what's in that plant, and we've established procedures for that through our local emergency planning committee that they can come in and see all that. But to have it out in the open arena, we've sort of gone away from the thoughts that we don't want people to be able to search around there for the best case or where they can maximize the most damage on the Internet, but we have still established ways that people can find that information out by visiting us or calling us, and we'll work with them on a one-on-one basis.

But for somebody to call up right now, what would concern me is you get a general call from somebody that says, I'd like a list of all your chemical plants and all your chemical plants that have these following chemicals. That kind of a request would be very

suspicious to us right now, and we wouldn't honor that request, but a legitimate request from a resident or a particular government official or something along those lines, we would make any and all of our information still available to them.

Mr. LISCOUSKI. Mr. Turner, thank you.

And I probably have the easiest answer in this space than anyone does, but I do that out of compassion for my colleagues, because from a pure protective standpoint I prefer we share no information with the general public. If we could prevent people in the open-source world from gaining access to information which could be used to exploit vulnerabilities, I'm all over that, and if I was at the one end of the spectrum to suggest that's what we ought to do, I'm here to tell you that I'm mandated, I'm charged with trying to protect the critical infrastructure of the United States, and that's a tool in the tool kit.

Now, I say that, but by the same token I know that my colleagues at the local level have to live in that space, and not having information really hampers their ability to do that. We're not going to prescribe how we share information or what the local officials share with their constituency and the population. As Chief Full pointed out, they can do that, they live with that, they live in the local area, they know the locals, they can talk with folks, they can share information responsibly.

It's a national problem, but there's no Federal answer for this at the local level to respond to it. But I can tell you that it's my concern that we do protect information that can be exploited by terrorist groups and others that are looking to do us harm.

Mr. HEADLEY. If I might just add one thing, if you're talking about availability of information, on February 13th I downloaded the TRI data on this facility from the Internet, which tells you all the quantities—the reporting here was 2001, it's not the most recent information, but if someone is interested in what chemicals are at that facility, it's widely available.

Mr. MURPHY. OK. Thank you, Mr. Chairman.

Mr. SHAYS.

Mr. SHAYS. Thank you. Maybe the best way to spend my time is to understand EPA's role and DHS's role. I don't really quite understand it. I don't understand whether the EPA has any role over the terrorist threat, and if not I need to know why, so maybe you can start me out.

Mr. LISCOUSKI. Sure. Let me start by describing what DHS's role here is vis-a-vis the Homeland Security Act and then how that's evolved or how we got to the Homeland Security Act and what that means to DHS and then how that's evolving in the context of providing security in cooperation with EPA.

Homeland Security Act 2002 established DHS——

Mr. SHAYS. Can you move the mic closer.

Mr. LISCOUSKI. Excuse me, sir. I'm sorry.

The Homeland Security Act of 2002 established DHS as the lead agency for chemical security in the chemical sector and in partnership with the EPA we're pursuing that. And that was a balance between safety and security. We did not assume the responsibilities for safety for which DHS—EPA—has the clear mandate, and the legislative and regulatory authority for safety programs are crucial,

as we're discussing here, to providing good foundation for security. You cannot separate those two things. But the responsibility for security for DHS, it was never intended to be a separate or mutually exclusive responsibility that moved to DHS without the cooperation of the EPA. We can't do that. I would never support it.

If the law provided for that I would quickly develop the relationships that I needed within the EPA to draw upon their expertise in this area because they have that domain expertise. Good government doesn't mean we should replicate responsibilities; good government means that we leverage responsibilities and capabilities across our government and that's precisely what we're doing with the EPA.

We work closely with the EPA to understand what the threats are, understand the priorities and, most importantly, the solutions and the remedies to the vulnerabilities.

To extend the Homeland Security Act 2002 which was effectively a strategy for what good nationwide homeland security is, the Homeland Security Presidential Directive No. 7, just recently signed by President Bush in December, is how we have to do those responsibilities collectively.

We're in the process of developing those, the tactics behind that strategy and the partnerships between the respective agencies that have responsibilities for all critical infrastructure; we're in dialog and constant negotiation with these agencies, and specifically with EPA, determining how we broker the respective responsibilities for ensuring we have protection for chemical, as well as the Department of Transportation who has authority in this area, as well as TSA and the Coast Guard who have authority in this area.

So we're taking a very holistic look at an end-to-end sort of perspective for chemical security effective at the ports, in transit, and ultimately in place at the sites themselves. So that has a responsibility broad spectrum across, as I pointed out, EPA, Coast Guard, DFT, TSA, DHS at a greater role, and probably a couple others that are not coming to mind.

So this is intended to be a very well-coordinated effort. DHS has responsibility in the context of actually doing the tactical things as well as the strategic responsibility of coordinating our efforts nationwide.

Mr. SHAYS. There's no Federal law evidently that explicitly requires all chemical facilities to take security actions to safeguard their facilities against terrorist attack.

Do you think this is wise and, if so, why?

Mr. LISCOSKI. Well, MTSA is responsible for the act enabling the Coast Guard with their oversight role in this area for the ports by virtue gives the Coast Guard that authority in part.

And working with the Coast Guard and, as I pointed out, with DOT, we believe that, you know, we can always make improvements; but we believe we can exploit the current regulatory authorities within those respective agencies to achieve a national level of security as it relates to chemical security.

Mr. SHAYS. How does the Coast Guard impact us here.

Mr. LISCOSKI. Well, with the two citations here, both of these sites, both in Neville Island and in Forward Township, are TSA, sir.

Mr. SHAYS. Maybe you gentlemen can explain it to me.

Mr. LISCOUSKI. I can amplify it if you like.

Mr. SHAYS. I must be out of my territory. I want to know, we don't have Federal laws that require the chemical plants to do security and I'm trying to ask if this made sense, and you're telling me that, you know, the Coast Guard—through the Coast Guard we somehow are getting chemical plants to do this.

So are you saying that they have requirements or they don't have requirements?

Mr. LISCOUSKI. No, I'm saying they do have requirements. The MTSA, the Maritime—

Mr. SHAYS. So you disagree with the statement. You think our laws now require chemical plants to secure their facilities.

Mr. LISCOUSKI. Within certain parameters, sir. The Coast Guard has mandated vulnerability assessments based upon standards to be provided to them by December 2003. We're in the process of collecting those standards currently. So under the MTSA—

Mr. SHAYS. That's for all chemical plants.

Mr. LISCOUSKI. No, those that fall within the purview of the MTSA, sir. That's what I was saying. This is a holistic approach, some of which are covered by regulations, some of which are covered by oversight by DHS.

You're asking for one—I think you're asking, do we need one single Federal law for security risk to chemical plants.

Mr. SHAYS. [Nods affirmatively.]

Mr. LISCOUSKI. Then I would say at this point in time, I think, working with the administration, I would say all things are on the table, but I'm not in a position to worry about that.

What I'm in a position to worry about is what's the security currently and what are we doing to improve that, and I'm telling you right now we're taking a very active approach to it.

Mr. SHAYS. I'm not trying to get you in a position where you're telling me what the administration has to do for policy, but I basically conclude you're the person in charge. The EPA has basically decided, fairly late, not to participate.

I'm trying to understand, you know, who's in charge if anyone in terms of what kind of absolute mandates we can make on chemical plants and whether we should, and I've seen two folks locally and I'm just trying to think, you know, what information is being shared with them. And I know there's a reluctance on the part of you to overstate or even understate the challenge. I'd like to get something out of this hearing that I can go home with and say, well, we need to move in this direction or that direction.

You're not giving me the opportunity to draw on your expertise to know whether you think that more Federal law is necessary, or some Federal law. You're telling me how you're coping and, you know, I mean, maybe that's the way we end this hearing, but it's not a very satisfying one from my standpoint in trying to learn something.

I'm trying to understand—I mean, for instance, I'm near a nuclear power plant. They have to have an evacuation plan, they have to determine where the plume goes and the probability of the plume, they have to have requirements for safety, and maybe it's

a bad comparison, maybe we just don't need it, but I think if we have it for nuclear plants why not for chemical?

So I thought maybe in this hearing I'd learn that, but maybe I've got to ask someone else. I don't know, it's getting to be a bit frustrating because I feel like I'm in a game. I just want to know some answers.

Gentlemen, tell me, do you have evacuation plans for neighborhoods around the chemical plants?

Mr. HEADLEY. As part of the improvements that we made at Vopak we came up with an evacuation plan for an accidental release, which obviously would apply for an intentional release as well, which essentially was to put in a warning siren, to send information to the people in the neighborhood and downstream to warn them that there was a problem. It's one of those things where you stay in place and put plastic over your windows and do that kind of thing until the threat dissipates.

Beyond that, I can't comment about the regulatory or who has ultimate authority on these matters because I just don't know.

Mr. SHAYS. Chief.

Chief FULL. My experience—and, again, the chemical facility and the Forward Township being in my county I can tell you that they are more the exception than the rule.

Mr. SHAYS. What's more the exception than the rule.

Chief FULL. What they have accomplished, both at the company level and with the municipality through their efforts, have been nothing less than extraordinary and outstanding in the spirit of cooperation. However, they are only 1 of 230 facilities I have in my county right now, and I am concerned about the fact that we don't have something. And, quite frankly, at this point in time at the local level, I don't care where it comes from, but there has to be something to improve the accountability for security of the facilities.

As I take a look at what we've discussed here this morning, I'm in the business of responding to those things when they have occurred; and with that, we've got to ensure that it doesn't occur and we can't be shopping around with who's going to do it under one regulation, I mean, we already are mandated under a number of different regulations that either come out of EPA or FEMA or something along those lines.

We, too, have a power plant 10 miles from here and I'm very familiar with what you've experienced with your power plant, and we have evacuation plans for our chemical facilities, as is required under our EPA reporting and so forth. But they have nothing to do—there's not one thing in there about security; it really doesn't even ask, do you have a site security plan? We have everything for consequence purposes, responding to if there's an emergency, but there is nothing to do with security at all, there's—and—

Mr. SHAYS. Mr. Liscouski, why wouldn't we just give the EPA that same responsibility and I'll just give you the analogy that I have. I mean, under FEMA they have natural disasters and they have man-made disasters and they respond to both and they deal with both.

Why would we separate that? Why wouldn't we just keep the EPA involved with the same—I mean, logically what is the argument for not doing it?

Mr. LISCOUSKI. I can only speak to what is, sir; I can't talk about the retrospective reasons as to why people made decisions.

I'll just tell you that when we talk about the responsibility for coordinating across the national picture for infrastructure protection and security, it makes sense that DHS has the responsibility to do that, working with our Federal partners.

Now, we talk about legislation and we talk about regulation, I think it's important to note, and we talk about things that have to be done at a minimum. As it relates to security, one of the things I'm always fearful of when people talk about legislation that deals with regulation is that it goes up to the fence line and typically deals with minimum standards.

When we talk about minimums here we're often talking about those things which don't meet a dynamic threat environment. The world that we come from and the world that we all currently live in with respect to the September 11th—the post-September 11th world is one in which we have a great dynamic threat.

My fear is legislation can only move at a certain pace and if we require chemical companies to achieve a minimum, the minimums, then they will go to the minimum; and if the threat exceeds that minimum, are we going to wait to enact legislation which is going to then take them to the next level of a minimum standard which might respond to an evolutionary threat?

My job is to ensure that we have robust capabilities and thinking going on. So to that end, irrespective of legislation sitting in the hopper or not, regardless of what requirements there are to meet regulatory requirements, we regularly work with the chemical sector across the industry, associations, individual companies, to assess their vulnerabilities, to get them to work and make the investments they need to do the things that they need to do, and we check up with them.

That's not requiring a legislative mandate to do that. We're moving out on that now, we're making improvements, and I can tell you right now we're exceeding anything that I've seen on the table yet with respect to legislation. Now, are we making progress to my satisfaction in terms of getting all 4,000 sites done to the level that we need to? No. Is there enough money to do that right off the bat? I'm not so sure it's a question of money. It's a question of time. And this is an evolutionary problem. We have to attack it as much as we can.

But if you want to leave this hearing satisfied, I can only tell you right now that we are not sitting waiting for legislation, good thought, to be passed by the Congress or anyone else before we take action. We're very aggressive about it. We're moving out and we're reducing vulnerabilities.

I'd like to say we're touching all the points that we need to be. We can be doing a better job, but the public should not be thinking that DHS is waiting for guidance from anybody before we move out there.

We're working hard with the industry, we're pushing them hard. I suspect you're going to hear on the next panel from the American

Chemistry Council how hard we're pushing them, how hard we're working them, and I'm upsetting some people by doing that. Do I care if I upset them? No. Do I care about making sure we've got the right security for the United States? Yes. That's what I've got to answer to, sir, not about making sure I've got some regulation, but making sure we understand the vulnerabilities and that we've got the right protection programs.

Mr. SHAYS. Our job is oversight of DHS under the law. We have oversight of the Department of State and the Department of Defense, FEMA and all the parts there.

Our job is to look at programs to see if they're working well, and then part of it is to determine whether we have to rewrite laws. Our committee has come up with tremendous amounts of recommendations, some to the Department of Homeland Security, and in the process of hearings we learn things that we can then recommend. It's not your job to write the law, it's our job. I understand that.

Mr. LISCOUSKI. I agree.

Mr. SHAYS. But it's our job to understand if we're doing it the right way and the best way. Is this the best way? We bring people before us to learn that.

And so I am just wrestling right now—and I think you can think it's pretty logical, we have EPA, they have it for accidental, and yet we have testimony from two people locally that they have nothing now for security. And I'm wondering why it's better to have DHS do it than not just to have EPA just revise what they do to have it also under security.

And that's what I'm wrestling with, and I'm not trying to play a game with you or anybody else, I'm asking a logical question and I'm hearing your answer saying, well, we're doing the best we're doing, we're not waiting.

What I wanted to know is what is the logic of not having EPA do it. Tell me that, please. Is there logic or is it just a value judgment?

Mr. LISCOUSKI. No, I believe there's logic for this for the same reason the Transportation Security Administration was formed from the likes of FAA and where there was a security component beforehand.

I think there is some recognition that there is a difference between safety and security, that safety provides a good foundation for security programs, but security has to be within the responsibility of an organization whose mandate and primary focus is security for the United States. That's DHS.

Mr. SHAYS. So your point about transportation—and then I'm done—is what? I'm missing your point. You're speaking too quickly for me.

Mr. LISCOUSKI. Sorry.

Mr. SHAYS. What's your point about Department of Transportation? The analogy to what to what.

Mr. LISCOUSKI. Well, prior to September 11th, the Department of Transportation did have airline security within its mandate. And then subsequent to September 11 the Transportation Security Administration was formed to ensure that we had an even greater focus, and that focus was then transferred to—

Mr. SHAYS. We took Coast Guard from Transportation and we moved it to DHS, I understand that. I'm not suggesting we take EPA and give it to you. But the question is, are we now doing two separate things? They're both dealing with security, that one is dealing with national and you dealing with man-made causes, and I am just wondering why. That's what I'm wrestling with.

We didn't do it in other areas. We haven't brought FEMA in, and FEMA does both. And I don't understand why we're separating it. That's what I'm trying to understand. If you don't know the answer to it then that's fine.

Mr. LISCOUSKI. Perhaps I'm not being clear. I think I do know that answer. The FEMA responsibility, which is now Emergency Preparedness and Response, is not a security responsibility but a preparedness and response capability.

The security responsibilities we have in the DHS are across a number of different elements. The safety responsibility for EP&A remains at EP&A. EP&A really never had a very robust security capability. We're trying new security programs based upon solely safety forces.

The industry—the government would obviously serve in terms of what the Homeland Security Act provided for—felt that DHS was the appropriate place for a nexus for security as it relates to all of our critical infrastructure and specifically to the chemical sector.

So I think the answer is there, perhaps I'm just not articulating it correctly and I apologize for that, but I'd be happy to spend more time with you trying to get clarity on it.

Mr. SHAYS. The Department of Homeland Security legislation emanated from this committee. We had the very first hearing on it and I understand the genesis of the legislation. I still for the life of me don't understand why EPA is not more involved in the security side and that's what I don't understand.

I don't understand why these gentlemen know that they have emergency plans when it relates to natural causes, but somehow they don't have it for man-made problems. I don't for the life of me understand that and I know you're trying to answer, but I don't understand.

Thank you, Mr. Chairman.

Mr. MURPHY. Mr. Shays.

We will move on to the next panel now. I thank you for your testimony, I appreciate it very much.

Mr. LISCOUSKI. Thank you, Mr. Chairman.

[Recess.]

Mr. MURPHY. All right. We'll continue now with our hearing and ask that the people about to give testimony please rise and be sworn.

[Witnesses sworn.]

Mr. MURPHY. I note for the record that the witnesses responded in the affirmative.

I'd like to introduce our panel, the second panel, for witnesses. These include Mr. John Stephenson, Director of National Resources and Environment for the U.S. General Accounting Office; Ms. Pamela Witmer, president of the Pennsylvania Chemical Industry Council; Mr. Marty Durbin, team leader for security and operations and senior director of Federal relations for the American Chemistry

Council; and we have Ms. Jennifer C. Gibson, vice president of government & public affairs, National Association of Chemical Distributors.

I welcome all the witnesses today to this hearing and I guess we'll begin with Mr. Stephenson, your testimony. Each person will get—

Mr. SHAYS. Five minutes.

Mr. MURPHY [continuing]. Five minutes and we'll roll over if we need to do that.

Mr. Stephenson.

STATEMENTS OF JOHN STEPHENSON, DIRECTOR OF NATIONAL RESOURCES AND ENVIRONMENT FOR THE U.S. GENERAL ACCOUNTING OFFICE; PAMELA WITMER, PRESIDENT OF THE PENNSYLVANIA CHEMICAL INDUSTRY COUNCIL; MARTY DURBIN, TEAM LEADER FOR SECURITY AND OPERATIONS AND SENIOR DIRECTOR OF FEDERAL RELATIONS FOR THE AMERICAN CHEMISTRY COUNCIL; AND JENNIFER C. GIBSON, VICE PRESIDENT OF GOVERNMENT AND PUBLIC AFFAIRS, NATIONAL ASSOCIATION OF CHEMICAL DISTRIBUTORS

Mr. STEPHENSON. Thank you, Mr. Chairman. Thank you for the opportunity to discuss our work on the security of the Nation's chemical facilities and the recommendations that we made to address this issue over a year ago in our March 2003 report.

As the events of September 11, 2001 showed, terrorists can cause enormous damage to our country by attacking infrastructure essential to our economy and jeopardizing public health and safety. Following these events, the President, in the National Strategy for Homeland Security, identified the chemical industry as 1 of 13 sectors critical to the Nation's infrastructure. Across the Nation, literally thousands of industrial facilities manufacture, use, or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk in the event of a chemical release.

The Federal Government's role in protecting chemical facilities from terrorist attacks has been much debated since September 11. Initially EPA had the lead responsibility for chemical security, but it has now been shifted to the new Department of Homeland Security, as you just heard. Public debate has centered on whether the Federal Government should impose security requirements on chemical facilities or whether voluntary industry actions alone are sufficient.

Let me briefly summarize the findings in our report. First, most experts agree that the Nation's chemical facilities are indeed attractive targets for terrorists intent on causing massive damage. The risk of an attack varies among facilities and upon several factors including the types of chemicals they use and their proximity to populated areas.

According to EPA data on accidental toxic release worst-case scenarios, as you heard, 123 chemical facilities located throughout the Nation could each potentially expose more than 1 million people in the surrounding area if a toxic release occurred, and another 700 facilities could each threaten at least 100,000 people.

Now, there's a chart in the back of our testimony that kind of in part explains the difference between those numbers and the 4,000 that DHS was talking about.

Numerous studies and media accounts of reporters gaining access to facilities indicates that the vulnerabilities are very real. Just a few months ago, as was already mentioned once here, the Pittsburgh Tribune Review did an expose on the vulnerability of such facilities in this area that CBS later used in a broader 60 Minutes piece on chemical plant security.

Despite the obvious risk, no Federal laws as yet explicitly require that all chemical facilities assess vulnerabilities or take security action to safeguard them from an attack. While some facilities must take action under recent legislation covering water treatment plants, part of those 15,000, or plants near ports, which is about 300 of those 15,000, no Federal regulation right now requires that all of them be assessed.

Furthermore, well over 2 years after the events of September 11 the Federal Government is still not comprehensive—has still not comprehensively assessed the chemical industry's vulnerability to terrorist attacks. EPA, the Department of Homeland Security, and the Department of Justice have each taken preliminary steps to assist the industry in its preparedness efforts, but no agency monitors or documents the extent to which chemical facilities have implemented security measures. Consequently, Federal, State and local entities in general lack information on preparedness.

To their credit chemical manufacturing industry associations have taken a number of voluntary initiatives to address security at their member facilities. For example, the American Chemistry Council, represented on this panel, requires its members to follow its responsible care approach and preparedness. ACC's efforts are commendable, but its members, while some of the Nation's biggest chemical companies, include less than 1,000 of the approximately 15,000 facilities the EPA estimates manufacture or store dangerous chemicals.

Relying on voluntary efforts alone without Federal oversight or third-party verification may not be sufficient to address the considerable threat. Indeed, relying on voluntary efforts alone raises serious concerns, and the extent the facilities are participating in such efforts is at this point unclear.

In light of the gravity of a potential threat and the obvious challenges facing the industry in addressing it, we recommended a year ago that the Department of Homeland Security and EPA jointly develop a comprehensive national strategy that, one, identifies high-risk facilities and collects information on preparedness—that sounds like that's partially being done according to the DHS witness; two, further specify the roles and responsibilities for addressing the threat; three, establish appropriate information sharing mechanisms; and, four, develop legislative proposals to require chemical facilities to expeditiously assess their vulnerability and, when necessary, make corrective actions.

Legislation is now working its way through the Congress that, if enacted, and I haven't seen the latest draft of this legislation, but would direct DHS and EPA to in part adopt most of these recommendations.

Mr. Chairman, that concludes the summary to my statement and I'll be happy to respond to questions at any time.

Mr. MURPHY. Thank you, Mr. Stephenson.

[The prepared statement of Mr. Stephenson follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security,
Emerging Threats, and International Relations,
Committee on Government Reform, House of
Representatives

For Release on Delivery
Expected at 9:30 a.m. EST
Monday, February 23, 2004

HOMELAND SECURITY

**Federal Action Needed to
Address Security
Challenges at Chemical
Facilities**

Statement of John B. Stephenson, Director
Natural Resources and Environment



G A O

Accountability * Integrity * Reliability

February 2004

HOMELAND SECURITY

Federal Action Needed to Address Security Challenges at Chemical Facilities



Highlights of GAO-04-482T, a testimony before the Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, House of Representatives

Why GAO Did This Study

The events of September 11, 2001, triggered a national re-examination of the security of thousands of industrial facilities that use or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk of serious injury or death in the event of a terrorist-caused chemical release. GAO was asked to examine (1) available information on the threats and risks from terrorism faced by U.S. chemical facilities; (2) federal requirements for security preparedness and safety at facilities; (3) actions taken by federal agencies to assess the vulnerability of the industry; and (4) voluntary actions the chemical industry has taken to address security preparedness, and the challenges it faces in protecting its assets and operations. GAO issued a report on this work in March 2003 (GAO-03-439).

What GAO Recommends

GAO's March 2003 report recommended that the Secretary of Homeland Security and the Administrator of EPA jointly develop a comprehensive national chemical security strategy that is both practical and cost effective, which includes assessing vulnerabilities to terrorist attacks and enhancing security preparedness.

Legislation is now before Congress that, if enacted, would direct DHS, or DHS and EPA, to adopt most of GAO's March 2003 recommendations.

www.gao.gov/cgi-bin/getpt?GAO-03-439.

To view the full report, including the scope and methodology, click on the link above. For more information, contact John B. Stephenson at (202) 512-3841 or stephensonj@gao.gov.

What GAO Found

Chemical facilities may be attractive targets for terrorists intent on causing economic harm and loss of life. Many facilities exist in populated areas where a chemical release could threaten thousands. The Environmental Protection Agency (EPA) reports that 123 chemical plants located throughout the nation could each potentially expose more than a million people if a chemical release occurred. To date, no one has comprehensively assessed the security of chemical facilities.

No federal laws explicitly require that chemical facilities assess vulnerabilities or take security actions to safeguard their facilities from attack. However, a number of federal laws impose safety requirements on facilities that may help mitigate the effects of a terrorist-caused chemical release. Although EPA believes that the Clean Air Act could be interpreted to require security at certain chemical facilities, the agency has decided not to attempt to require these actions in light of the litigation risk and importance of an effective response to chemical security. Ultimately, no federal oversight or third-party verification ensures that voluntary industry assessments of vulnerability are adequate and that security vulnerabilities are addressed.

Currently, the federal government has not comprehensively assessed the chemical industry's vulnerabilities to terrorist attacks. EPA, the Department of Homeland Security (DHS), and the Department of Justice have taken preliminary steps to assist the industry in its preparedness efforts, but no agency monitors or documents the extent to which chemical facilities have implemented security measures. Consequently, federal, state, and local entities lack comprehensive information on the vulnerabilities facing the industry.

To its credit, the chemical manufacturing industry, led by its industry associations, has undertaken a number of voluntary initiatives to address security at facilities. For example, the American Chemistry Council, whose members own or operate approximately 1,000, or 7 percent, of the facilities subject to Clean Air Act risk management plan provisions, requires its members to conduct vulnerability assessments and implement security improvements. The industry faces a number of challenges in preparing facilities against attacks, including ensuring that all chemical facilities address security concerns. Despite the industry's voluntary efforts, the extent of security preparedness at U.S. chemical facilities is unknown. In October 2002 both the Secretary of Homeland Security and the Administrator of EPA stated that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness. Legislation is now pending that would mandate chemical facilities to take security steps to protect against the risk of a terrorist attack.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on the security of the nation's chemical facilities and the recommendations that we made to address this issue in our March 2003 report.¹

As the events of September 11, 2001, showed, terrorists can cause enormous damage to our country by attacking infrastructure essential to our economy and jeopardizing public health and safety. Following these events, the President, in the National Strategy for Homeland Security, identified the chemical industry as one of 13 sectors critical to the nation's infrastructure. Across the nation, thousands of industrial facilities manufacture, use, or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk of injury or death in the event of a chemical release.

Even before September 11, 2001, protecting chemical facilities was the shared responsibility of federal, state, and local governments in partnership with the private sector. However, attention was focused largely on the risks of accidental, rather than intentional, chemical releases. Under the Clean Air Act, the Environmental Protection Agency (EPA) identified 140 toxic and flammable chemicals that pose the greatest risk to human health and the environment when present in certain quantities above threshold levels. According to EPA, approximately 15,000 facilities in a variety of industries produce, use, or store one or more of these chemicals beyond threshold amounts. Under the act, these facilities must take steps to prevent and prepare for an accidental chemical release, including developing risk management plans (RMP). These facilities are referred to as RMP facilities. The events of September 11, 2001, brought heightened attention to security at chemical facilities and the possibility of a chemical release caused by a terrorist attack.

The federal government's role in protecting chemical facilities from terrorist attacks has been much debated since September 11, 2001. Initially, EPA had the lead responsibility for chemical security; currently the Department of Homeland Security (DHS) is the lead federal agency. For both agencies, public debate has centered on whether the federal

¹U.S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, GAO-03-439 (Washington, D.C.: Mar. 14, 2003).

government should impose security requirements on chemical facilities or whether voluntary industry actions are sufficient. Several legislative proposals have been introduced that address security measures at chemical facilities, including provisions giving DHS, or EPA and DHS, authority to mandate security measures at chemical facilities.

My remarks today will focus on security preparedness at the nation's chemical facilities. In particular I will (1) summarize available information on the threats and risks from terrorism that U.S. chemical facilities face; (2) describe federal requirements for security preparedness and the safe management of chemicals at these facilities; (3) describe actions federal agencies have taken to assess the vulnerability of the chemical industry or to address security preparedness; and (4) describe voluntary actions the chemical industry has taken to address security preparedness, and the challenges it faces in protecting its assets and operations. Our 2003 report was based on our review of available reports, statutes and regulations, and industry association documents; interviews with officials from the Department of Defense, the Department of Justice, EPA, industry associations including the American Chemistry Council (ACC) and the Synthetic Organic Chemical Manufacturers Association (SOCMA), and other chemical industry officials; and selected chemical facility site visits. We limited our review to stationary chemical facilities and did not address security concerns surrounding transportation of hazardous chemicals.² Appendix I provides additional information on the processes covered under the Clean Air Act's for RMP facilities, by industry sector, and the residential population surrounding RMP facilities that could be threatened by a "worst-case" accidental chemical release.

Summary

In summary, experts agree that the nation's chemical facilities may be attractive targets for terrorists intent on causing massive damage, but the extent of security preparedness since the events of September 11, 2001, is unknown. The risk of an attack varies among facilities depending upon several factors, including their location and the types of chemicals they use, store, or manufacture. No specific data exist on the actual effects of successful terrorist attacks on chemical facilities. However, according to

²For information on the transportation of hazardous material, see U.S. General Accounting Office, *Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed*, GAO-03-435 (Washington, D.C.: April 2003) and U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 2003).

EPA data on accidental toxic release "worst-case" scenarios, 123 chemical facilities located throughout the nation could each potentially expose more than one million people in the surrounding area if a toxic release occurred. Approximately 700 facilities could each potentially threaten at least 100,000 people in the surrounding area, and about 3,000 facilities could each potentially threaten at least 10,000 people. To date, no one has comprehensively assessed the security of chemical facilities; however, numerous studies and media accounts of reporters and environmental activists gaining access to facilities indicate that vulnerabilities exist.

Unlike water treatment facilities and nuclear power facilities, chemical facilities are not subject to any federal requirements to assess and address security vulnerabilities against terrorist attacks. However, a number of federal laws impose safety requirements that may help mitigate the effects of a chemical release resulting from a terrorist attack. A case in point is the Clean Air Act's requirements that RMP facilities take safety precautions to detect and minimize the effects of accidental releases, as well as provide prompt emergency response to a release. Although EPA believes the Clean Air Act could be interpreted to require security actions at RMP facilities, the agency has decided not to attempt to require these actions in light of the litigation risk and importance of an effective response to chemical security. In addition, under the regulations for the Maritime Transportation Security Act of 2002, vessels and port facilities—some of which are chemical facilities—must develop security plans. However, no federal oversight or third-party verification ensures that voluntary industry assessments of vulnerability are adequate and that security vulnerabilities are addressed.

Currently, the federal government has not comprehensively assessed the chemical industry's vulnerability to terrorist attacks. As a result, federal, state, and local entities lack comprehensive information on the vulnerabilities the industry faces. However, federal agencies have taken some preliminary steps to assist the industry in its preparedness efforts. For example, EPA has issued warning alerts to the industry and informally visited about 30 high-risk facilities to learn about and encourage security efforts. According to EPA officials, EPA has provided information to DHS about the 15,000 facilities and DHS is currently identifying high-risk facilities and conducting site visits. In May 2002, Justice submitted an interim report to Congress that described observations on security at 11 chemical manufacturing facilities. As we reported in October 2002, however, Justice has not prepared a more comprehensive final report to Congress on the industry's vulnerabilities, which it was required by law to deliver in August 2002. In a February 2003 conference report on Justice's

appropriations, Congress directed that funding be transferred to DHS for completing vulnerability assessments at chemical facilities.

Finally, although the chemical industry has undertaken a number of initiatives to address security concerns, the extent of security preparedness across the chemical industry is unknown. The American Chemistry Council—whose 145 member companies own or operate approximately 1,000 (7 percent) of the 15,000 RMP facilities—now requires, as a condition of membership, that facilities conduct security vulnerability assessments and implement security improvements. EPA officials estimate that voluntary initiatives led by industry associations only reach a portion of the 15,000 RMP facilities. Moreover, the industry faces a number of challenges in preparing facilities against terrorist attacks, including ensuring that facilities obtain adequate information on threats and determining the appropriate security measures given the level of risk. In October 2002, both the Secretary of Homeland Security and the then-Administrator of EPA stated that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness. They also stated that they would support bipartisan legislation to require the 15,000 chemical facilities nationwide that contain large quantities of hazardous chemicals to comprehensively assess their vulnerabilities and then act to reduce them.

In light of the challenges facing the industry and the gravity of the potential threat, we recommended in March 2003 that the Secretary of Homeland Security and the Administrator of EPA jointly develop a comprehensive national strategy for chemical security that is both practical and cost effective. This national strategy should

- identify high-risk facilities based on several 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.

Legislation is now before Congress that, if enacted, would direct DHS, or DHS and EPA, to adopt most of these recommendations.

Background

Chemical facilities manufacture a host of products—including basic organic chemicals, plastic materials and resins, petrochemicals, and industrial gases, to name a few. Other facilities, such as fertilizer and pesticide facilities, pulp and paper manufacturers, water facilities, and refineries, also house large quantities of chemicals. EPA has a role in preventing and mitigating accidental releases at chemical facilities through, among other things, the RMP provisions of the Clean Air Act. Under these provisions, EPA identified 140 toxic and flammable chemicals that, when present above certain threshold amounts, would pose the greatest risk to human health and the environment if released. According to EPA, approximately 15,000 facilities in a variety of industries produce, use, or store one or more of these chemicals beyond threshold amounts.

The 2003 President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets sets forth actions that EPA and DHS will take to secure the chemical infrastructure. The strategy directs EPA and DHS to promote enhanced site security at chemical facilities and review current practices and statutory requirements on the distribution and sale of certain pesticides and industrial chemicals to help identify whether additional measures are necessary. DHS is also charged with continuing to develop the Chemical Sector Information Sharing and Analysis Center, a partnership with industry to facilitate the collection and sharing of threat information, by promoting the Center and recruiting chemical industry constituents to participate. A presidential directive issued in December 2003 designates DHS as the lead federal agency for chemical security, a change from national strategies issued in July 2002 and February 2003, which named EPA as the lead.

A number of other critical infrastructures have federal security requirements. All commercial nuclear power facilities licensed by the Nuclear Regulatory Commission are subject to a number of security requirements. The Aviation and Transportation Security Act of 2001 directed the Transportation Security Administration to take over responsibility for airport screening. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires community water systems serving more than 3,300 people to conduct a vulnerability assessment, prepare an emergency response plan, certify to EPA that the vulnerability assessment and emergency response plan have been completed, and provide a copy of the assessment to EPA. To improve security in our nation's ports, the regulations implementing the Maritime

Transportation Security Act of 2002 direct vessels and facilities—some of which are chemical facilities—to develop security plans.³

Congress is considering several legislative proposals that would grant DHS, or DHS and EPA, the authority to require chemical facilities to take security steps. S. 994 requires the Secretary of Homeland Security to promulgate regulations specifying which facilities should be required to conduct vulnerability assessments and to prepare and implement site security plans, a timetable for completing the vulnerability assessments and security plans, the contents of plans, and limits on the disclosure of sensitive information. S. 157 would direct EPA to designate high-priority chemical facilities based on the threat posed by an unauthorized release and require these facilities to conduct vulnerability assessments, identify hazards that would result from a release, and prepare a prevention, preparedness, and response plan. S. 157 would also require facilities to send these assessments and plans to EPA. EPA and DHS would jointly review the assessments and plans to determine compliance. S. 157 would also require that facilities consider inherently safer practices (referred to as inherently safer technologies), such as substituting less toxic chemicals.

An Attack Against Chemical Facilities Could Cause Economic Harm and Loss of Life

Experts agree that chemical facilities present an attractive target for terrorists intent on causing massive damage because many facilities house toxic chemicals that could become airborne and drift to surrounding areas if released. Chemical facilities could also be attractive targets for the theft of chemicals that could be used to create a weapon capable of causing harm. Justice has concluded that the risk of an attempt in the foreseeable future to cause an industrial chemical release is both real and credible. In fact, according to Justice, domestic terrorists plotted to use a destructive device against a U.S. facility that housed millions of gallons of propane in the late 1990s. In testimony on February 6, 2002, the Director of the Central Intelligence Agency warned of the potential for an attack by al Qaeda on chemical facilities.

Some chemical facilities may be at higher risk of a terrorist attack than others because they contain large amounts of toxic chemicals and are located near population centers. Attacks on such facilities could harm a

³In responding to our draft, EPA noted that approximately 2,000 RMP facilities may be covered under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

large number of people, with health effects ranging from mild irritation to death, cause large-scale evacuations, and disrupt the local or regional economy. No specific data are available on what the actual effects of successful terrorist attacks on chemical facilities would be. However, RMP facilities must submit to EPA estimates, including the residential population located within the range of a toxic gas cloud produced by a "worst-case" chemical release, called the "vulnerable zone." According to EPA, 123 chemical facilities located throughout the nation have toxic "worst-case" scenarios where more than one million people could be at risk of exposure to a cloud of toxic gas.⁴ About 600 facilities could each potentially threaten between 100,000 and a million people, and about 2,300 facilities could each potentially threaten between 10,000 and 100,000 people within these facilities' "vulnerable zones."

According to EPA, "worst-case" scenarios do not consider the potential causes of a release or how different causes or other circumstances, such as safety features, could lessen the consequences of a release. Hence, the "worst-case" scenario calculations would likely be overstating the potential consequences. However, under the Clean Air Act, RMP facilities must estimate the effects of a toxic chemical release involving the greatest amount of the toxic chemical held in a single vessel or pipe—not the entire quantity on site. Therefore, for some facilities it is conceivable that an attack where multiple chemical vessels were breached simultaneously could result in an even larger release, potentially affecting a larger population than estimated in the RMP "worst-case" scenarios. Other factors besides location and the quantity of chemicals onsite could also make a facility a more attractive target. For example, a facility that is widely recognizable, located near a historic or iconic symbol, or critical to supporting other infrastructures could be at higher risk. A 2002 Brookings

⁴"Vulnerable zones" are determined by drawing a circle around a facility with the radius of the circle equal to the distance a toxic gas cloud would travel before dissipating to relatively harmless levels. Because, in an actual event, the toxic cloud would only cover a fraction of that circle, it is unlikely that the event would actually result in exposure of the entire population estimated in the "worst-case" scenario, according to EPA. The number of persons within a "vulnerable zone" is larger than the number of persons that would be affected by a "worst-case" scenario. In addition, EPA's requirements for "worst-case" release analysis tend to result in consequence estimates that are significantly higher than what is likely to actually occur. For example, "worst-case" release analysis does not take into account active mitigation measures facilities often employ to reduce the consequences of releases.

Institution report ranks an attack on toxic chemical facilities behind only biological and atomic attacks in terms of possible fatalities.⁴

Currently, no one has comprehensively assessed security across the nation at facilities that house chemicals. According to a 1999 study by the Department of Health and Human Services' Agency for Toxic Substances and Disease Registry (ATSDR), security at chemical facilities in two communities was fair to very poor. ATSDR observed security vulnerabilities such as freely accessible chemical barge terminals and chemical rail cars parked near residential areas in communities where facilities are located. Following visits to 11 chemical facilities, Justice concluded that some facilities may need to implement more effective security systems and develop alternative means to reduce the potential consequences of a successful attack. The ease with which reporters and environmental activists gained access to chemical tanks and computer centers that control manufacturing processes at chemical facilities in recent years also raises doubts about security effectiveness at some facilities.

No Federal Requirements Specifically Require Chemical Facilities to Address the Threat of Terrorism

No federal laws explicitly require all chemical facilities to take security actions to safeguard their facilities against a terrorist attack. Although the federal government requires certain chemical facilities to take security precautions directed to prevent trespassing or theft, these requirements do not cover a wide range of chemical facilities and may do little to actually prevent a terrorist attack. For example, under EPA's regulations implementing the Resource Conservation and Recovery Act of 1976, facilities that house hazardous waste generally must take certain security actions, such as posting warning signs and using a 24-hour surveillance system or surrounding the active portion of the facility with a barrier and controlled entry gates.⁵ However, according to EPA, these requirements would be applicable to only approximately 21 percent of the 15,000 RMP facilities. Regulations implementing the Maritime Transportation Security Act of 2002 also require vessels and port facilities—some of which are chemical facilities—to develop security plans.

⁴The Brookings Institution, *Protecting the American Homeland: A Preliminary Analysis*, (Washington, D.C.: 2002).

⁵40 C.F.R. § 264.14.

A number of federal laws also impose safety requirements on chemical facilities, but these requirements do not specifically and directly address security preparedness against terrorism. Several statutes, including the Occupational Safety and Health Act, the Clean Air Act, and the Emergency Planning and Community Right-to-Know Act, impose safety and emergency response requirements on chemical facilities that may incidentally reduce the likelihood and mitigate the consequences of terrorist attacks.⁷ All of these requirements could potentially mitigate a terrorist attack in a number of ways. First, because some of these requirements only apply to facilities with more than threshold quantities of certain chemicals, facility owners have an incentive to reduce or eliminate these chemicals, which may make the facility a less attractive target or minimize the impact of an attack. Second, both the Clean Air Act risk management plan provisions and the hazard analyses under the Occupational Safety and Health Act require facility operators to identify the areas of their facilities that are vulnerable to a chemical release. When facilities implement measures to improve the safety of these areas, such as installing sensors and sprinklers, the impact of a terrorist-caused release may be lessened. Third, the emergency response plans increase preparedness for a chemical release—whether intentional or unintentional. While these safety requirements could mitigate the effects of a terrorist attack, they do not impose any security requirements, such as conducting vulnerability assessments and addressing identified problems.

While no law explicitly requires facilities to address the threat of terrorism, EPA believes that the Clean Air Act could be interpreted to provide it with authority to address site security from terrorist attacks at chemical facilities. Section 112(r) of the Clean Air Act—added by the Clean Air Act Amendments of 1990—imposes certain requirements on chemical facilities with regard to “accidental releases.” The act defines an accidental release as an unanticipated emission of a regulated substance or other extremely hazardous substance into the air. Arguably, any chemical release caused by a terrorist attack would be unanticipated and thus could be covered under the Clean Air Act. An interpretation of an unanticipated emission as including an emission due to a terrorist attack would provide EPA with authority to require security measures or vulnerability assessments with regard to terrorism. However, EPA has not

⁷We focus our discussion in this testimony on those requirements dealing with assessments of hazards and emergency response. However, the Toxic Substances Control Act also may mitigate the consequences of a terrorist attack by limiting or eliminating certain toxic chemicals that a facility manufactures or uses.

attempted to use these Clean Air Act provisions. EPA is concerned that such an interpretation would pose significant litigation risk. As we reported in March 2003, there are a number of practical and legal arguments against this interpretation. We find that EPA could reasonably interpret its Clean Air Act authority to cover chemical security, but also agree with the agency that this interpretation could be open to challenges. At the time of our 2003 review, EPA supported passage of legislation to specifically address chemical security.

**Federal Agencies
Have Not
Comprehensively
Assessed the
Vulnerability of the
Chemical Industry to
Terrorism, but Have
Taken Some
Preliminary Steps**

Despite a congressional mandate to do so, the federal government has not conducted the assessments necessary to develop comprehensive information on the chemical industry's vulnerabilities to terrorist attacks.⁸ The Chemical Safety Information, Site Security and Fuels Regulatory Relief Act of 1999 required Justice to review and report on the vulnerability of chemical facilities to terrorist or criminal attack. In May 2002, nearly 2 years after it was due, Justice prepared and submitted an interim report to Congress that described observations on security at 11 chemical manufacturing facilities Justice visited to develop a methodology for assessing vulnerability, but its observations cannot be generalized to the industry as a whole. In its fiscal year 2003 budget, Justice asked for \$3 million to conduct chemical plant vulnerability assessments. In the February 2003 conference report on Justice's appropriation act for fiscal year 2003,⁹ Congress directed that \$3 million of the funding being transferred to DHS to be used for the chemical plant vulnerability assessments. Justice believes that chemical plant vulnerability assessments are now part of DHS' mission.

Federal agencies have taken preliminary steps to assist the industry in its preparedness efforts. While Justice has not assessed the vulnerability of the chemical industry, it has provided the industry with a tool for individual facilities to use in assessing their vulnerabilities. Justice, together with the Department of Energy's Sandia National Laboratories, developed a vulnerability assessment methodology for evaluating the vulnerability to terrorist attack of facilities handling chemicals. The

⁸For a discussion on Justice's actions to assess the chemical industry's vulnerability to terrorist attack, see U.S. General Accounting Office, *Homeland Security: Department of Justice's Response to Its Congressional Mandate to Assess and Report on Chemical Industry Vulnerabilities*, GAO-03-24R (Washington, D.C.: Oct. 10, 2002).

⁹H.R. Conf. Rept. No. 103-10, at 600 (2003).

methodology helps facilities identify and assess threats, risks, and vulnerabilities and develop recommendations to reduce risk, where appropriate. As the lead federal agency for the operational response to terrorism, Justice's FBI is responsible for weapons of mass destruction threat assessment and communicating warnings. Finally, agents in the FBI's local field offices provide information and technical assistance to state and local jurisdictions and to some chemical facilities to bolster their preparedness to respond to terrorist incidents.

EPA has also taken some actions. Officials have analyzed the agency's database of RMP facilities to identify high-risk sites for DHS and Justice's Federal Bureau of Investigation (FBI). But these facilities are only a portion of the universe of all industrial facilities that house toxic or hazardous chemicals. At the time of our review, EPA had not analyzed non-RMP facilities to determine whether any of those facilities should be considered at high risk for a terrorist attack. EPA has also issued warning alerts to the industry, hosted training classes on vulnerability assessment methodologies, and informally visited about 30 high-risk facilities to learn about and encourage security efforts. Finally, DHS' Information Analysis and Infrastructure Protection directorate collects information from the U.S. intelligence community, other federal agencies, and the private sector. Working with ACC, an industry association representing chemical manufacturers, DHS also supports the Chemical Sector Information Sharing and Analysis Center to collect and share threat information for the chemical industry. In addition, according to EPA officials, DHS has begun identifying high-risk facilities and conducting site visits at facilities. However, neither EPA nor DHS is currently monitoring the extent to which the industry has implemented security measures.

**Chemical Industry
Has Taken Voluntary
Actions to Address
Security Concerns but
Faces Significant
Challenges in
Preparing Against
Terrorist Attacks**

The chemical manufacturing industry has undertaken a number of voluntary initiatives to address security concerns at chemical facilities, including developing security guidelines and tools to assess vulnerabilities, but major challenges remain. All of the industry groups with whom we met have taken actions such as forming security task forces, holding meetings and conferences to share security information with members, and participating in security briefings with federal agencies. In response to the terrorist attacks on September 11, 2001, ACC—whose members own or operate approximately 1,000 RMP facilities—now requires its members, as a condition of membership, to rank facilities using a screening tool to evaluate its facilities' risk level. It also requires facilities to identify, assess, and address vulnerabilities at facilities using one of several available

vulnerability assessment methodologies. In doing so, ACC member facilities generally follow a multistep process that includes

- evaluating on-site chemical hazards, existing safety and security features, and the attractiveness of the facility as a terrorist target;
- using hypothetical threat scenarios to identify how a facility is vulnerable to attack; and
- identifying security measures that create layers of protection around a facility's most vulnerable areas to detect, delay, or mitigate the consequences of an attack.

ACC established time frames for completing the vulnerability assessment and implementing security measures, based on the facility's risk ranking. ACC reports that the 120 facilities ranked as the highest risk and 372 facilities ranked as the next highest have completed vulnerability assessments. Most of ACC's lower-risk facilities are progressing on schedule. ACC generally requires third-party verification that the facility has made the improvements identified in its vulnerability assessment.¹⁰

While these are commendable actions, they do not provide a high level of assurance that chemical facilities have better protected their facilities from terrorist attack. First, ACC does not require third parties to verify that the facility has conducted the vulnerability assessment appropriately or that its actions adequately address security risks. Even though compliance with ACC's safety and security requirements is a condition of membership, we do not believe that its requirements for facilities to periodically report on compliance with these requirements is an effective enforcement measurement because ACC does not verify implementation or evaluate the adequacy of facility measures. Second, its member facilities comprise only 7 percent of the facilities required to submit risk management plans to EPA, leaving about 14,000 other RMP facilities that may not participate in voluntary security efforts. These facilities include agricultural suppliers, such as fertilizer facilities; petroleum and natural gas facilities; food storage facilities; water treatment facilities; and wastewater treatment facilities, among others. Third, other facilities house

¹⁰The lowest-risk facilities may use a less rigorous methodology to identify and make security enhancements and are not required to obtain third-party verification that improvements have been made. In addition, by December 2005, member companies will have to had their compliance with safety and security requirements certified by independent third-party auditors.

chemicals that EPA has identified as hazardous, but in quantities that are below the threshold level required to be categorized as RMP facilities.

Other industry groups are also developing security initiatives, but the extent of these efforts varies from issuing security guidance to requiring vulnerability assessments. For example, the American Petroleum Institute, which represents petroleum and natural gas facilities, published security guidelines developed in collaboration with the Department of Energy that are tailored to the differing security needs of industry sectors. Despite industry associations' efforts to encourage security actions at facilities, the extent of participation in voluntary initiatives is unclear. EPA officials estimate that voluntary initiatives led by industry associations only reach a portion of the 15,000 RMP facilities. Furthermore, EPA officials stated that these voluntary initiatives raise an issue of accountability, since the extent to which industry group members are implementing voluntary initiatives is unknown.

The chemical industry faces a number of challenges in preparing facilities against terrorist attacks, including ensuring that facilities obtain adequate information on threats and determining the appropriate security measures given the level of risk. Trade association and industry officials identified a number of concerns about preparing against terrorist attacks. First, industry officials noted that they need better threat information from law enforcement agencies, as well as better coordination among agencies providing threat information. Second, industry officials report that chemical companies face a challenge in achieving cost-effective security solutions, noting that companies must weigh the cost of implementing countermeasures against the perceived reduction in risk. Industry groups with whom we spoke indicated that their member companies face the challenge of effectively allocating limited security resources. Third, facilities face pressure from public interest groups to implement inherently safer practices (referred to in the industry as inherently safer technologies), such as lowering toxic chemical inventories and redesigning sites to reduce risks. Justice has also recognized that reducing the quantity of hazardous material may make facilities less attractive to terrorist attack and reduce the severity of an attack. While industry recognizes the contribution that inherently safer technologies can make to reducing the risk of a terrorist attack, industry officials noted that decisions about inherently safer technologies require thorough analysis and may shift, rather than reduce, risks. Finally, industry officials stated that the industry faces a challenge in engaging all chemical facilities in voluntary security efforts. ACC has made efforts to enlist facilities beyond its membership in voluntary security initiatives. The Synthetic Organic

Chemical Manufacturers' Association (SOCMA) adopted ACC's security code for its member facilities as a condition of membership. However, the extent to which all partnering companies and associations implement the requirements is unclear.

Mr. Chairman, this concludes my prepared statement. I would be happy to respond to any questions that you or Members of the Subcommittee may have.

**Contacts and
Acknowledgements**

For further information about this testimony, please contact me at (202) 512-3841. Joanna Owusu, Vince Price, Carol Herrnstadt Shulman, and Amy Webbink made key contributions to this statement.

Appendix I: RMP-Covered Industrial Processes and Off-Site Consequences of Worst-Case Chemical Releases

This appendix presents information on the processes covered under the Clean Air Act's requirements for risk management plan (RMP) facilities by industry sector and the residential population surrounding RMP facilities that could be threatened by a "worst-case" accidental chemical release.

Table 1: Number and Percent of RMP-Covered Processes by Industry Sector

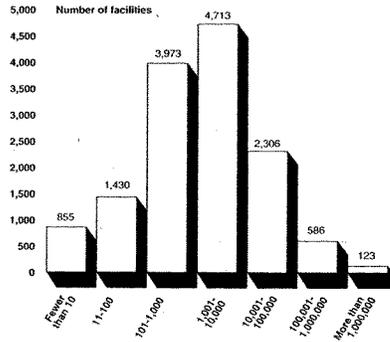
Industry sector	Number of processes	Percent of processes
Agriculture & farming, farm supply, fertilizer production, pesticides	6,317	31
Water supply and wastewater treatment	3,753	18
Chemical manufacturing	3,803	18
Energy production, transmission, transport, and sale	3,038	15
Food and beverage manufacturing & storage (including refrigerated warehousing)	2,366	11
Chemical warehousing (not including refrigerated warehousing)	318	2
Other*	1,075	5
Total†	20,670	100

Source: EPA

*Other represents a large variety of industry sectors including pulp mills, iron and steel mills, cement manufacturing, and computer manufacturing.

†The total number of covered processes is not equal to the 15,000 RMP facilities because some RMP facilities have more than one covered process (i.e., a process containing more than a threshold amount of a covered hazardous chemical).

Figure 1: Number of Facilities with Worst-Case Accidental Release Scenarios by Residential Population Potentially Threatened



Source: EPA.

Notes: EPA, Chemical Accident Risks in U.S. Industry – A Preliminary Analysis of Accident Risk Data from U.S. Hazardous Chemical Facilities, Washington, D.C.: September 25, 2000.

This figure includes only those facilities with toxic chemicals that could lead to a "worst-case" scenario. Facilities that only have flammable chemical "worst-case" scenarios are not included. Flammable chemicals affect fewer people because the distance the flammable substance travels tends to be significantly shorter.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs**Contact:**

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

Mr. MURPHY. Ms. Witmer.

Ms. WITMER. Good morning, Mr. Chairman and members of the House Subcommittee on National Security, Emerging Threats and International Relations. As Congressman Murphy indicated, my name is Pam Witmer and I am president of the Pennsylvania Chemical Industry Council. PCIC represents over 70 companies involved in the manufacture, distribution, and use of chemicals along with those companies that support our industry.

Pennsylvania's business of chemistry is an approximately \$27 billion a year industry employing almost 62,000 Pennsylvanians. These jobs represent over 8 percent of the Commonwealth's entire manufacturing work force, a work force that takes home on average over \$68,000 a year.

I'm pleased to appear before you today to discuss the efforts that have been undertaken post September 11 by those involved in Pennsylvania's chemical industry. We are committed to work in partnership with Federal, State and local governments to further ensure the security of materials that are used to make everyday products like Kevlar for bulletproof vests for our military and law enforcement, water purification systems, bicycle helmets for our children, siding and insulation for our homes and lifesaving medicines. Hazardous materials are used to make the products that drive our economy and contribute to our well-being. It is equally important to understand that of the hazardous materials manufactured and transported, only a small portion of them would be considered attractive to a would-be terrorist.

The chemical industry has long taken security seriously. In this "just in time" culture it's imperative that materials are moved from manufacturer to customer in a timely, efficient, cost-effective and secure manner. As well, the industry has made it a priority to establish a good working relationship with members of the local first-response community.

I think the key word used to describe the industry's security efforts to date is "proactive." Efforts to further enhance security through formal industrywide guidelines were undertaken immediately following the tragic events of September 11th. Shortly following 9/11, industry had developed, distributed and began training on the use of the Site Security Guidelines for the Chemical Industry. These guidelines were followed by the more comprehensive American Chemistry Council Responsible Care Security Code. These documents were developed jointly by the American Chemistry Council, CHEMTREC, the Chlorine Institute, the Synthetic Organic Chemical Manufacturers Association, and subsequently supported by many other chemical industry associations including the Pennsylvania Chemical Industry Council.

PCIC supports efforts to pass Federal legislation that would place authority for establishing national standards for chemical site security and overseeing their implementation with the Department of Homeland Security. PCIC also suggests that such Federal legislation recognize the ACC Responsible Care Security Code as an acceptable security standard. PCIC does not support individual States acting on their own in absence of Federal legislation.

From PCIC's perspective there are three themes essential to the successful development and implementation of a security plan: use of sound science and actual risk posed, outreach and training.

Sound science and actual risk. The Site Security Guidelines and the more recent Security Code represent 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. The Guidelines and Security Code were written specifically for those who have responsibility for the safe and secure management and distribution of their products and raw materials. The Responsible Care Security Code outlines a tiered risk-based approach to identifying vulnerabilities and implementing security programs and practices that managers can consider and tailor to a company's specific situation as identified in vulnerability assessment. The two documents offer flexibility to design a program according to the chemical being used and the actual risk posed.

Some of the more obvious strategies being employed include changing the direction trucks enter a facility, use of employee identification cards, background checks for employees and contractors, additional surveillance in the forms of obvious cameras as well as placement of more covert cameras, additional fencing, more security guards, etc.

As I mentioned, these are some of the obvious methods employed to better secure the sites that manufacture, store, use and distribute hazardous materials. Actual security plans are, of course, confidential and, on the advice of law enforcement, not discussed.

The second element of a successful security plan is outreach and information sharing. Hazardous materials security is a shared responsibility. It is not just the job of government agencies, law enforcement or a particular industry sector. It is all of these groups working together that would provide the best opportunity to prevent or respond appropriately to an act of terrorism, international or domestic.

Information sharing is a critical element for effective security. Along with understanding the real risk posed by a particular chemical, being provided with accurate information can trigger heightened or tightened security.

This shared responsibility extends to those involved in the manufacture and distribution of chemicals. A number of initiatives have been established that do enable government agencies, law enforcement, and various industry sectors to interact on information sharing. Some of these efforts include the Chemical Sector Sharing and Analysis Center. In April 2002, ACC and the National Infrastructure Protection Center, which was then part of the FBI, signed a formal agreement establishing a communications network that operates 24 hours a day to provide an exchange of security and threat information between the Federal Government, the chemical manufacturers, carriers and distributors. PCIC is also a subscriber of the Chemical Sector ISAC to ensure that chemical manufacturers and distributors not affiliated with ACC are provided with the latest security and threat information.

Some of the other advances in information sharing include the Railroad Alert Network, the Surface Transportation Information

Sharing and Analysis Center, the Chemical Transportation Emergency Center and the Association of American Railroads and the American Chemistry Council Security Task Force.

As you can see, much has been done in the way of providing better access to information. However, there still exists a reluctance to pass along critical intelligence because of the sensitive nature of the intelligence or its source. Consideration should be given by the Federal Department of Homeland Security to developing a process that would provide top security clearance for certain chief security executives within companies, as many of these individuals come from the intelligence or law enforcement community.

The third theme of all hazardous materials security efforts, training, is essential. PCIC member companies participate in drills to determine whether or not the plan is effective, sharpen skills and responses and to determine what needs to be done better.

An example of a cooperative training effort that took place this past November was the national level terrorism-related preparedness drill involving the U.S. Coast Guard, the FBI, PCIC member company ConocoPhillips and State and local law enforcement agencies for Pennsylvania and New Jersey. This particular training exercise utilized a scenario involving a simulated terrorism-induced oil spill in the Delaware River to test the Unified Command's capability to respond to a breach in port security while at the same time containing and responding to a major oil spill.

PCIC and many of our member companies also voluntarily participate in and support a national organization called TransCAER, which stands for Transportation Community Awareness Emergency Response. Pennsylvania TransCAER is a unique organization that counts among its members the Federal Environmental Protection Agency, the Federal Emergency Management Agency, the Pennsylvania Emergency Management Agency, the Pennsylvania Department of Transportation and the Keystone Emergency Management Association, in addition to chemical manufacturers, distributors and hazardous materials cleanup companies. Pennsylvania TransCAER, an award-winning affiliate of the national TransCAER organization, has as its mission, outreach and training to communities in which our facilities are located and through which our materials are transported.

Pennsylvania TransCAER has just completed its second consecutive year of providing free hazardous materials incident response training to county and local first responders. This unique training utilizes actual scenes from within the county in which the training is being held, allows first responders to role play all elements of a hazardous materials transportation incident, from the initial call reporting the incident, to managing the incident, to cleanup, to reporting relevant information to medical and hospital personnel, to working with the media.

I am pleased to announce this voluntary effort will be offered free to an additional seven Pennsylvania counties in 2004. Allegheny County was one of the first counties to be offered this free training in 2002 and neighboring Beaver County participated in the Pennsylvania TransCAER training event in 2003.

On a more local level, many employees of PCIC member companies are active participants in their county's Terrorism Task Force.

They are volunteer firefighters or emergency medical technicians. As well, some of our member companies have agreements with their local emergency planning coordinator that allow the company's hazardous materials response team to go offsite and assist in a hazardous materials emergency.

This unprecedented information sharing, outreach and training is taking place not just between law enforcement and industry, but also with other Federal and State agencies. An example of this cooperation on a national level is the industry's participation in a Federal Department of Transportation study that is currently underway to field test various new technologies that may be beneficial for tracking shipments of hazardous materials under a variety of scenarios. PCIC is a member of the security discussion group created by Pennsylvania's Homeland Security Director, Keith Martin.

As you can see, the manufacturer and distribution of hazardous materials is more secure today than it was last year and certainly more secure than it was 5 or 10 years ago.

This does not mean that we are done nor does it mean that there will never be a successful terrorist attack. It does mean that we recognize our responsibility to try and secure our employees and communities through which our materials are transported and manufactured.

A number of positive and proactive voluntary initiatives have already been taken to develop more secure movement of hazardous materials. Research will continue looking for better ways to improve approaches to security that are based on sound science and developed on the basis of actual risk. But society as a whole faces the problem that in response to all types of threats, terrorism, natural disasters, etc., in general there is no such thing as zero risk. Whether it's airports, water treatment plants, high-rise buildings or hazardous materials, we must all realize there are real costs to every person for each effort made to reduce the likelihood of risks negatively impacting us.

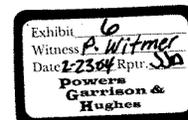
I realize I went way over my time, but thank you and whenever it's appropriate I'll answer questions.

Mr. MURPHY. Thank you.

[The prepared statement of Ms. Witmer follows:]



Pennsylvania Chemical Industry Council
200 N. Third Street, 10th Fl.
Harrisburg, PA 17101



717.232.6681
717-232.4684
www.pcic.org

**House Subcommittee on National Security, Emerging Threats, and International Relations,
Committee on Government Reform
Combating Terrorism: Chemical Plant Security Hearing
Moon Township Municipal Building
Moon Township, PA
February 23, 2004**

Good morning Mr. Chairman and members of the House Subcommittee on National Security, Emerging Threats and International Relations. My name is Pam Witmer. I am president of the Pennsylvania Chemical Industry Council. (PCIC) PCIC represents over 70 companies involved in the manufacture, distribution, and use of chemicals along with those companies that support our industry.

Pennsylvania's business of chemistry is an approximately \$27 billion a year industry employing almost 62,000 Pennsylvanians. These jobs represent over eight percent of the Commonwealth's entire manufacturing workforce, a workforce that takes home on average over \$68,600 a year.

I am pleased to appear before you today to discuss the efforts that have been undertaken post 9/11 by those involved with Pennsylvania's chemical industry. We are committed to work in partnership with federal, state, and local governments to further ensure the security of materials that are used to make everyday products like Kevlar® for bullet proof vests for our military and law enforcement, water purification systems, bicycle helmets for our children, siding and insulation for our homes and life saving medicines. Hazardous materials are used to make the products that drive our economy and contribute to our well-being. It is equally important to understand that of the hazardous materials manufactured and transported, only a small portion would be considered "attractive" to a would-be terrorist.

The chemical industry has long taken security seriously. In this "just in time" culture, it is imperative that materials are moved from manufacturer to customer in a timely, efficient, cost-effective and secure manner. CHEMTREC®, which I will discuss in more detail later, is an example of the industry's long standing commitment to secure the movement of hazardous materials. As well, the industry has made it a priority to establish a good working relationship with members of the local first response community.

I think the key word used to describe the industry's security efforts to date is – proactive. Efforts to further enhance security through formal industry-wide guidelines were undertaken immediately following the tragic events of September 11th. Shortly following 9/11, industry had developed, distributed, and began training on the use of the Site Security Guidelines for the

Chemical Industry. These guidelines were followed by the more comprehensive American Chemistry Council Responsible Care® - Security Code. These documents were developed jointly by the American Chemistry Council (ACC), CHEMTREC®, the Chlorine Institute, the Synthetic Organic Chemical Manufacturers Association (SOCMA), and subsequently supported by many other chemical industry associations including the Pennsylvania Chemical Industry Council.

PCIC supports efforts to pass federal legislation that would place authority for establishing national standards for chemical site security and overseeing their implementation with the Department of Homeland Security. PCIC also suggests that such federal legislation recognize the ACC Responsible Care® Security Code as an acceptable security standard. PCIC does not support individual states acting on their own in the absence of federal legislation.

There are three themes central to the successful development and implementation of a security plan: use of sound science and actual risk posed, outreach, and training.

Sound Science and Actual Risk

The Site Security Guidelines and the more recent Security Code represent 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. The Guidelines and Security Code were written specifically for those who have responsibility for the safe and secure management and distribution of their products and raw materials. The Responsible Care® Security Code outlines a three-tiered risk based approach to identifying vulnerabilities and implementing security programs and practices that managers can consider and tailor to a company's specific situation as identified in the vulnerability assessment. The documents offer flexibility to design a program according to the chemical being used and the actual risk posed.

Some of the more obvious strategies being employed include:

- Changing the direction trucks enter a facility;
- Use of employee identification cards;
- Background checks for employees and contractors;
- Additional surveillance in the form of obvious cameras as well as the more covert; and
- Additional fencing, more security guards, etc.

As I mentioned these are some of the obvious methods employed to better secure the sites that manufacture, store, use and distribute hazardous materials. Actual security plans are of course, confidential, and, on the advice of law enforcement are not discussed.

Outreach and Information Sharing

Hazardous materials security is a shared responsibility. It is not just the job of government agencies, law enforcement or a particular industry sector. It is all of these groups working together that will provide the best opportunity to prevent or respond appropriately to an act of terrorism, international or domestic. Information sharing is a critical element to effective security. Along with understanding the real risk posed by a particular chemical, being provided with accurate information can trigger heightened or tightened security.

This shared responsibility extends to those involved in the manufacture and distribution of chemicals. A number of initiatives have been established that do enable government agencies,

law enforcement, and various industry sectors to interact on information sharing. Some of these efforts include:

- Chemical Sector Information Sharing and Analysis Center (ISAC) – In April 2002, ACC and the National Infrastructure Protection Center (then part of the FBI) signed a formal agreement establishing a communications network that operates 24-hours a day to provide an exchange of security and threat information between the federal government and chemical manufacturers, carriers, and distributors. PCIC is also a subscriber of the Chemical Sector ISAC to ensure that chemical manufacturers and distributors not affiliated with ACC are also provided with the latest security and threat information.
- Railroad Alert Network (RAN) – The rail industry and the chemical industry work cooperatively on the exchange of information that is pertinent to the secure movement of hazardous materials by rail.
- Surface Transportation Information Sharing and Analysis Center (ST ISAC) – The ST ISAC operates similarly to the Chemical Sector ISAC and is open to all providers and users of surface transportation.
- Chemical Transportation Emergency Center (CHEMTREC®) – CHEMTREC® has been in operation since 1972. Operating “24/7”, it employs individuals qualified to assist emergency responders involved in virtually any type of emergency involving hazardous materials. CHEMTREC® maintains the world’s largest electronic database of Material Safety Data Sheets. (MSDSs) In addition, if the circumstances warrant, CHEMTREC® staff can establish communications between a very large network of chemical and hazardous materials experts, CHEMTREC® personnel and the responders at the scene of the incident.
- *Association of American Railroads and the American Chemistry Council Security Task Force* – An inter-industry task force designed to discuss and make recommendations to address security issues of interest to both groups. The three primary areas of work for the task force are: communications, plant access and storage-in-transit.

As you see much has been done in the way of providing better access to information, however, there still exists a reluctance to pass along critical intelligence because of the sensitive nature of the intelligence or its source. Consideration should be given the federal Department of Homeland Security to developing a process to provide top security clearance for certain chief security executives within companies. Many of these individuals come from the intelligence and law enforcement community.

Training

The third theme of all hazardous materials security efforts – training – is essential. PCIC member companies participate in drills to determine whether or not the plan is effective, sharpen skills and responses, and to determine what needs to be done better.

An example of a cooperative training effort that took place this past November was the national-level terrorism related preparedness drill involving the U.S. Coast Guard, the FBI, PCIC member company ConocoPhillips, and state and local law enforcement agencies from Pennsylvania and New Jersey. This particular training exercise utilized a scenario involving a simulated terrorism-induced oil spill in the Delaware River to test the Unified Command’s capability to respond to a breach in port security while at the same time containing and responding to a major oil spill.

PCIC and many of our member companies also voluntarily participate in and support a national organization called TransCAER® which stands for Transportation Community Awareness Emergency Response. PA TransCAER® is a unique organization that counts among its members the federal Environmental Protection Agency, the federal Emergency Management Agency, the Pennsylvania Emergency Management Agency, the Pennsylvania Department of Transportation, and the Keystone Emergency Management Association (county emergency coordinators) in addition to chemical manufacturers, distributors and hazardous materials cleanup companies. PA TransCAER®, an award winning affiliate of the national TransCAER® organization, has as its mission outreach and training to communities in which our facilities are located and through which our materials are transported.

PA TransCAER® has just completed its second consecutive year of providing free hazardous materials incident response training to county and local first responders. This unique training, utilizing actual scenes from within the county in which the training is being held, allows first responders to role-play all elements of a hazardous materials transportation incident from the initial call reporting the incident to managing the incident to cleanup to reporting relevant information to medical and hospital personnel to working with the media.

I am pleased to announce that this voluntary effort will be offered free to an additional seven Pennsylvania counties in 2004. The counties selected for the 2004 training are: Berks, Cambria, Carbon, Erie, Lackawanna, Montgomery, and Northampton. I would like to point out that Allegheny County was one of the first counties to be offered this free training in 2002 and Beaver County participated in the PA TransCAER® training event in 2003.

On a more local level, many employees of PCIC member companies are active participants in their county's Terrorism Task Force, they are volunteer firefighters, or are emergency medical technicians. (EMTs) As well, some of our member companies have agreements with their local emergency planning coordinator (LEPC) that allow the company's hazardous materials response team to go off site and assist in a hazardous materials emergency.

This unprecedented information sharing, outreach, and training is taking place not just between law enforcement and industry, but also with other federal and state agencies. An example of this cooperation on a national level is the industry's participation in a federal Department of Transportation study that is currently underway to field test various new technologies that may be beneficial for tracking shipments of hazardous materials under a variety of scenarios. PCIC is a member of security discussion group created by Pennsylvania's Homeland Security Director, Keith Martin.

As you can see, the manufacture and distribution of hazardous materials is more secure today than it was last year and certainly more secure than it was five or ten years ago. Transporters and facilities have assessed their risk and are working to enhance plans to address those vulnerabilities. Information sharing is occurring on a level not previously seen. Training and drilling are involving all the appropriate groups.

This does not mean that we are done, nor does it mean that there will never be a successful terrorist attack. It does mean that we recognize our responsibility to try and secure our employees and communities through which our materials are transported and manufactured. Nationally the chemical industry is four and a half times safer than all other industries. This long held positive record on safety has translated into the chemical industry being further ahead than

many industries in the area of transportation security. A number of positive, proactive, and voluntary initiatives have already been developed to better secure hazardous materials. Research will continue; looking for better ways to improve approaches to security that are based on sound science and developed on the basis of actual risk. But society as a whole faces the problem that in response to all types of threats, terrorism, natural disasters, etc., in general there is no such thing as zero risk. Whether it is airports, water treatment plants, high-rise buildings, or hazardous materials we must all realize there are real costs to every person for each effort made to reduce the likelihood of risks negatively impacting us. Some of these costs are too high because they will impair our quality of life and livelihoods. As I stated earlier, hazardous materials security is a shared responsibility and the next steps must be developed collaboratively to make the most sense.

Thank you for the opportunity to provide you with an outline of some of the proactive and voluntary activities undertaken by Pennsylvania's business of chemistry and the industry nationally to better secure hazardous material. I would be happy to answer any questions you may have.

Mr. MURPHY. Mr. Durbin.

Mr. DURBIN. Good morning. Again, my name is Marty Durbin and on behalf of the members of the American Chemistry Council I certainly appreciate the opportunity to address security in the business of chemistry, a critical sector of America's infrastructure.

ACC represents 140 of the leading companies in the U.S. Chemical manufacturing industry. It's an industry with the largest exporting sector in our economy directly employing a million people and is the largest private industry investor in research and development. Products we manufacture are essential to our modern lives, from plastics to pharmaceuticals, from cars to clothing, and they keep our drinking water safe, support agriculture and spur medical innovations that prevent and treat disease.

Now, you've asked that we address voluntary actions the chemical industry has taken to address security and assess the Federal Government's roles and programs in this area. I welcome the opportunity to highlight three specific areas. One is the leadership role that I believe ACC members have taken with regard to security to further ensure the security and safety of their products facilities and the communities in which they operate; and, second, the strides the Federal Government has made in the last year in this area; and, third, the remaining challenges and where we need to go from here.

As has been mentioned several times, safety and security have been primary concerns of this industry since long before September 11th; however, those attacks forced every part of America's critical infrastructure to reevaluate security preparedness. Our members didn't wait for government direction. Building on the ethic of stewardship embodied in our trademark Responsible Care Program now in its 16th year, our members acted swiftly, adopting an aggressive plan to further enhance security, and that is the ACC Responsible Care Security Code.

Through the code, ACC members are making serious commitments and significant investments. Implementation of the code, which addresses site, cyber and transportation security is mandatory for all members. Regarding facilities specifically, the code requires that for every facility in all four categories, a rigorous security vulnerability assessment be conducted, security enhancements are implemented, and that a third party verify that those enhancements have indeed taken place.

The code emphasizes that security is a shared responsibility requiring actions by others in order to be effective. That includes suppliers and customers as well as government agencies, first responders law enforcement and everyone else we've been speaking about this morning.

The ACC Security Code has been called a model program by Secretary Ridge, and, as Mr. Stephenson mentioned, in the GAO report last year it was commended. More recently the Code was recognized by the U.S. Coast Guard, by the State of New Jersey, and by the city of Baltimore as essentially a best practice for chemical security. I'd be happy to go into more detail on that during the question period.

ACC's efforts, of course, extend far beyond the boundaries of just our facilities. We understand that effective response systems are

key to safety and security and, as such, we have longstanding public service programs such as CHEMTREC, which we mentioned earlier, a 24-hour emergency response center that has now been a public service of the American Chemistry Council for over 30 years, and the TransCAER program, again, as Ms. Witmer discussed.

The GAO report last year said that ACC's efforts were commendable, but we have not been content to rest on our laurels. Our members have continued to push themselves to strengthen our partnerships with law enforcement, first responders as well as local, State and Federal Government, and to meet the ambitious timetable of our security code. I'm pleased to report that our members are meeting their timetable. Every member facility has completed a vulnerability assessment and with many enhancements already in place we're on a path to full implementation of security enhancements by the end of this year.

Now, second, regarding the Federal Government and its role, We've been working very closely with the Department of Homeland Security during its first year of existence. We concurred with GAO's recommendations last year that the Federal Government should develop a comprehensive national chemical security strategy that's both practical and cost effective and that would focus in the following four areas.

First, identifying high-risk facilities. Now, I can tell you that starting in March of last year DHS partnered with ACC and Mr. Liscouski mentioned much of that in his testimony. Today DHS and the Coast Guard are actively visiting chemical facilities and working in conjunction with local law enforcement and responders to protect facilities and their communities.

In addition it's worth noting that U.S. Customs has developed the Customs Trade Partnership Against Terrorism program [CTPAT], to help identify potentially vulnerable or suspect shipments and works with manufacturers and shippers through the value chain, both foreign and domestic, to secure global trade.

Second, GAO identified the need to specify the roles and responsibilities of Federal agencies. Since their report was published, and as has already been mentioned, the President signed a Presidential Directive in December that more clearly defines security roles of various Federal agencies and specifically names DHS as the lead agency for the chemical sector.

Third was the need to develop appropriate information sharing mechanisms. As has been mentioned, the FBI through the National Infrastructure Protection Center contacted ACC shortly after September 11th and asked that we sponsor and host the chemical sector ISAC and through our CHEMTREC program we provide that 24/7 capability for a direct two-way communication between DHS and our sector to hundreds of participants representing not only our members but other segments of the chemical sector as well.

I would also note that while the national terrorist threat level was at orange during December and January, DHS established daily contact with ACC and its member companies to maintain a clear understanding of threats and countermeasures that were taken.

Finally, GAO recommended developing a legislative proposal, and here I want to be very clear that the members of ACC fully

recognize that strengthening safety and security and having Federal oversight at our facilities is in the best interest of our plant communities, our companies and our Nation.

As such, ACC supports chemical security legislation that will establish national guidelines for security at chemical facilities, require facilities to conduct vulnerability assessments and implement security plans, provide oversight and inspection authority to the Department of Homeland Security and create strong enforcement authority.

Now, we've been very pleased with the constructive relationships we're developing with our Federal partners to address the security in the chemical sector, and frankly Assistant Secretary Liscouski is to be commended for the focus that he personally has brought to this effort; however, I will confirm what he's telling you, that he is certainly going to great lengths to push our members in our industry to do even more than they are to help develop and establish what this higher level of sustainable security is at our member companies. But we look forward to working with our government partners to continuously enhance security of our products, our facilities, our employees and our communities.

Although much has been done there are areas in which we must continue to focus our attention, and they include improved public/private intelligence sharing regarding threats and vulnerabilities, coordinated training activities, improved coordination of chemical security initiatives within DHS and all of its various agencies, and agreement on other security needs of the chemical sector. And I'm pleased to say the dialog in all of these areas is underway.

In conclusion, I want to say that security is a responsibility shared by industry and government. ACC members will continue to step up to their security responsibilities; however, we know we can't do this alone.

Our members have already invested hundreds of millions of dollars to further enhance security, but unilateral security investment by the private sector is not enough.

ACC members will continue to work with law enforcement, first responders and government partners to ensure the security of our essential products and contributions this industry provides to our country. We demonstrated our commitment and willingness to step up to this challenge, but we cannot shoulder the burden alone. We need to embrace a more comprehensive and more integrated partnership with our public sector colleagues. Frankly, security is just not an option for the members of the American Chemistry Council.

Thank you, again. I'm happy to answer your questions at the appropriate time.

Thank you, Mr. Durbin.

[The prepared statement of Mr. Durbin follows:]



STATEMENT OF MARTIN J. DURBIN

SECURITY TEAM LEADER

THE AMERICAN CHEMISTRY COUNCIL

Testimony before the

**HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND
INTERNATIONAL RELATIONS**

**Moon Township Municipal Building
1000 Beaver Grade Road
Moon Township, PA 15108**

FEBRUARY 23, 2004

Good morning. My name is Marty Durbin, and I am the Security Team Leader 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 140 members of the American Chemistry Council 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 possible. 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 so critical in so many aspects of American life, including keeping our drinking water safe, supporting agriculture, spurring medical innovations to prevent and treat disease.

The ACC represents the leading companies in the U.S. chemical manufacturing industry, an industry which is the largest exporting sector in the economy (\$91 billion), employs one million people in America alone, with \$460 billion in sales. 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, you have asked us to address voluntary actions the chemical industry has taken to address security, and to assess the federal government's roles and programs in this area. I welcome the opportunity to highlight three things for you and the committee: 1) the leadership role ACC members have taken to further ensure the safety and security of their products, their facilities, and the communities in which they operate and the effective partnerships we are building with all levels of government, first responders, and law enforcement; 2) the great strides the federal government has taken in the last year to assure the security of the chemical sector; and 3) the progress and

challenges remaining, including the need for national legislation to provide an appropriate federal government oversight role over chemical sector security.

I. ACC's Leadership Role in Enhancing the Security of the Chemical Sector

Safety and security have been primary concerns of ACC members since long before September 11, 2001. However, the attacks on America that day forced every part of America's critical infrastructure to reevaluate security preparedness. Our member companies did not wait for government direction following September 11th. Building on the ethic of stewardship embodied in our trademark Responsible Care® program – now in its 16th year – our members acted swiftly, adopting an aggressive plan to further enhance security for our facilities, our communities, and our products – ACC's Responsible Care® Security Code.

Through the Security Code, ACC members are making serious commitments to enhance security, including security against a potential terrorist attack at plant sites, with customers and suppliers throughout the supply chain, and through cyber systems. Implementation of this Security Code according to a strict timeline is mandatory for all members of the American Chemistry Council.

Long before September 11, 2001, the chemical industry was working on facility security guidelines. But the tragic events of that day hastened the completion of facility, transportation and cyber security guidelines designed to help companies continuously improve their security at plant sites and throughout their businesses. The Security Code emphasizes that security is a shared responsibility requiring actions by others as well, such as suppliers and government agencies in order to be effective. By working with state and local governments, federal agencies like the Department of Homeland Security (DHS), law enforcement, and first responders, ACC members are developing relationships with key partners to strengthen the security of the nation's chemical sector.

How the ACC Responsible Care® Security Code Works

- **Prioritization and Assessment of Sites.** Companies prioritized their plant sites into one of four tiers based on three factors – potential consequences of a successful attack, difficulty of an attack, and attractiveness of the target – with Tier 1 sites being the highest priority for immediate security assessment. Once prioritized, Security Vulnerability Assessments were performed at all ACC-member facilities by the end of last year. ACC members were required to use rigorous methodologies developed by Sandia National Laboratories, the Center for Chemical Process Safety (part of the American Institute of Chemical Engineers) or an equivalently rigorous and robust method.
- **Implementation of Security Measures.** Once vulnerability assessments were completed, companies began implementing security measures commensurate with the vulnerabilities identified in the assessments. (See attachment-1 for representative enhancements.)
- **Protecting Information and Cyber-Security.** Protecting information and information systems is a critical component of a sound security management system and an essential part of the Security Code. This includes evaluating potential vulnerabilities in facility process control systems as well as corporate information technology systems and taking appropriate measures to address vulnerabilities identified.
- **Training, Drills and Guidance.** Emergency preparedness remains a hallmark of Responsible Care® implementation. For over 20 years, ACC member facilities have worked closely with one another and local responders to develop local emergency response and mutual assistance plans. Those existing response plans and relationships form an invaluable basis for the next generation of security response plans and the training and joint drills that are critical for local readiness. Training is not limited to responders, however, all facility employees will receive training in security awareness and reporting procedures. The eyes of our employees are invaluable safety assets and will likewise become invaluable security assets.
- **Communications, Dialogue and Information Exchange.** Communications with stakeholders is an important part of the Security Code. This dialogue and information exchange on appropriate security issues, balanced with safeguards for sensitive information, helps employees, contractors, communities, customers, suppliers, service providers and government officials and agencies be partners in enhancing security.
- **Response to Security Threats and Incidents.** Companies are to evaluate, respond, report and communicate security threats as appropriate. Facilities develop security programs that can be increased at higher threat levels and address factors such as access control, restricted areas, cargo handling, and monitoring.
- **Independent Third-Party Verification.** Companies will undergo an independent third-party verification at chemical operating facilities with potential off-site impacts.

This process will verify that companies have implemented the physical site security measures to which they have committed.

- **Continuous Improvement.** Extending continuous performance improvement guidelines beyond environment, health and safety, the Security Code includes planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.
- **Timing of the Security Code.** Responsible Care companies must implement security enhancements at the highest priority sites by December 31, 2003. Security enhancements at all sites are to be implemented by December 31, 2004. Implementation of the full Code for sites, transportation and cyber is due by June 30, 2005. Timing for security vulnerability assessments, security enhancements and verifications are below. (Attachment 2)

Our members' efforts are not limited to facility security. ACC members are also obligated to perform vulnerability assessments and implement countermeasures regarding their value chain (suppliers/distribution partners/customers) and cyber systems (process control and other information technology.) Every employee involved in the transportation of hazardous materials is required by federal regulation to undergo specific training relating to safety and security. Chemical companies have augmented those requirements with their own transportation security practices that build on existing safety training. 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.

ACC's Security Code has been called a model program by Secretary Ridge. In its report last March, the GAO praised the efforts our industry has taken: "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."¹

¹GAO, "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."

More recently, the U.S. Coast Guard recognized the Responsible Care® Security Code as an Alternative Security Program (RCSC - ASP) under the Maritime Transportation Security Act (MTSA) for purposes of fulfilling facility security regulatory requirements under 33 CFR 105. The Responsible Care® Security Code was the first alternative security program the Coast Guard has approved for facilities; most others have been for vessels. In addition, the State of New Jersey has recognized the Code as a “best practice” for chemical facility security, and is working on a “Memorandum of Agreement” that recognizes the Responsible Care® Security Code as an alternative to a regulatory regime. In addition, the City of Baltimore adopted a security ordinance that recognizes the Responsible Care® Security Code as an alternative means of compliance.

The President’s *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003) not only recognized the chemical industry’s vital contributions to America’s economy and lifestyle, but emphasized the crucial need for “meaningful information sharing” between the federal government and the private sector owners and operators of critical infrastructure. ACC and its member companies are working 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 keep DHS well-informed about the security measures our member companies implement at different threat levels, so DHS has an increasingly accurate picture of our security preparedness. And we have established secure procedures for reporting suspicious activities to DHS. These initiatives were formalized in an agreement between the federal government and ACC in April 2002 when the Chemical Sector Information Sharing and Analysis Center (ISAC) was established, allowing for two-way direct communication of threat information and incident reports between DHS and the hundreds of ISAC participants.

ACC's ethic of stewardship extends far beyond the boundaries of our facilities. We understand that effective response systems are key to safety and security. ACC members have long recognized that safety and emergency response are shared responsibilities and have a long tradition of coordinated emergency response and mutual assistance networks in communities. Chemical companies have created mutual response networks to bring to bear the best resources available to respond to those incidents. Additionally, our industry has instituted public service programs such as the CHEMTREC[®] and TRANSCAER[®] programs to assist public responders and local communities.

CHEMTREC[®] is a 24-hour-a-day emergency communications center, which has been operated as a public service of the American Chemistry Council 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. The TRANSCAER[®] program, which stands for "Transportation Community Awareness and Emergency Response," is a national effort that links the chemical industry, transportation organizations and local emergency response services. Through a network of regional and state coordinators, the TRANSCAER[®] program works with many local communities to help them better understand the movement of hazardous materials and how to respond to a transportation incident should one occur.

To facilitate exchange of information and lessons learned among industry security professionals, ACC and the Synthetic Organic Chemical Manufacturers Association (SOCMA) co-sponsor an annual 2-day Chemical Security Summit. Over 300 people attended last year's summit to discuss issues ranging from facility vulnerability assessment to cargo security; identifying countermeasures to communicating with the public. The Summit also provides an outstanding opportunity for security vendors to make their products and services known within the chemical sector.

Mr. Chairman, GAO's report last year said that "ACC's efforts are commendable," but, as you can see, we have not been content to rest on our laurels. Our members have continued to push themselves, to strengthen our partnerships with law enforcement and first responders, as well as local, state and federal government, and to meet the ambitious timetable of our Responsible Care[®] Security Code. I'm pleased to report that our members are meeting that timetable. Approximately 120 Tier I facilities completed SVAs by the end of 2002, and since GAO's report came out last March, 372 Tier II, 510 Tier III facilities and 950 Tier IV facilities have all completed SVAs. Tier I facilities were required to complete implementation of their security enhancements by 12/31/03, and those enhancements will be verified by outside third parties by March 31st.

II. The Federal Government Has Made Great Strides in Enhancing Security of the Chemical Sector

As I have indicated, ACC and its members have been working closely with the Department of Homeland Security during its first year of existence. We concurred with GAO's recommendations last year 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."

Identify High Risk Facilities

Starting in March 2003 DHS partnered with ACC to facilitate visits to member facilities. Information gained from these visits supports the development of targeted DHS and state efforts to provide support and resources to facilities and communities. ACC also worked with the DHS to develop methods for evaluating facilities based on potential physical and economic consequences. And even before the creation of DHS, Coast Guard, State offices of Homeland Security or Counter-Terrorism visited facilities to offer advice on enhancing facility security.

Today, DHS' Protective Security Division and the Coast Guard are actively visiting chemical facilities, reviewing SVAs and security plans, understanding common vulnerabilities and developing plans, in conjunction with local law enforcement and responders, to protect facilities and their communities.

ACC supports the work done by U.S. Customs Service as it developed the Customs-Trade Partnership Against Terrorism to help identify potentially vulnerable or suspect shipments and work with manufacturers and shippers through the value chain – both foreign and domestic – to secure global trade.

Specify the Roles and Responsibilities of Federal Agencies

Since the GAO report was published, the organizational roles and responsibilities of the federal agencies have become increasingly clear. In December, 2003, the President issued a directive -- *Homeland Security Presidential Directive 7* – clearly defining roles for various federal agencies, and specifically naming DHS as the lead agency for the chemical sector.

Through the Coast Guard's Maritime Transportation Security efforts over 4000 facilities – many of them ACC members – are developing explicit security plans to prevent and address transportation security incidents. All facility and vessel plans are to be in place by June 30 of this year. Individual facility plans will include schedules for employee security training and response drills and exercises. The plans will include

explicit 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. Even more facilities will participate in the development of and be covered by Area Port Security plans.

Develop Appropriate Information Sharing Mechanisms

Soon after 9/11 the FBI contacted ACC to sponsor and host an “Information Sharing and Analysis Center” between the government and the chemical sector. CHEMTREC stood up the Chemical Sector ISAC in April 2002. The ISAC has 578 participants representing not only ACC members, but other segments of the chemical sector. The Chemical Sector ISAC provides 24-7 capability for the Homeland Security Operations Center (HSOC) to contact the chemical sector as well as the ability 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. DHS also facilitates communications between infrastructure sectors – sectors that are mutually dependent on one another. Building on the success of the Chemical Sector ISAC, ACC is in the process of more formally organizing the Chemical Sector and facilitating a “Chemical Sector Coordinator” contact for DHS.

In addition, DHS recently finalized the Critical Infrastructure Information Act rules, which will provide the necessary protections for sensitive information to enhance information sharing between the private sector, the federal government, and state and local governments. The rules will improve key parties’ understanding of the threats, vulnerabilities and countermeasures affecting their localities, while ensuring that the information cannot fall into the wrong hands.

Communication During Raised Alert Level

While the national terrorist threat level was at “Orange” last December and January, DHS established daily contact with ACC and its member companies to maintain

a clear understanding of threats and countermeasures taken. A small group of industry security experts have been available as a resource to DHS 24/7.

Develop a legislative proposal

ACC continues to support federal oversight of chemical security. We realize this is in the best interest of our plant communities, our companies, and our nation. And ACC has repeatedly affirmed its support for responsible legislation.

The members of the ACC fully recognize that strengthening safety and security AND having federal oversight at our facilities is in the best interest of our nation. As such, ACC supports chemical security legislation that will:

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

In addition to legislation, the following things are essential to our ability to continuously enhance the security of our products, our facilities, our employees and our communities.

We need:

- Improved public/private intelligence sharing regarding threats and vulnerabilities
- Improved Emergency Response coordination and training
- Improved coordination of chemical security initiatives regarding facility, transportation, cyber, and product security within DHS; and
- Agreement on other security needs of the chemical sector, including a common understanding of what constitutes the US chemical sector and its interdependencies with other critical infrastructure sectors.

Conclusion

Security is a responsibility shared by industry and government. ACC members will continue to step up to our security. However, we know we can't do this alone. Our members invested millions of dollars last year to enhance security at their facilities, but unilateral security investment by the private sector is not enough.

The members of the American Chemistry Council will continue to work with law enforcement, first responders, and state and federal regulators to find the best solutions ensuring the security of the essential products and contributions this industry provides to our country. ACC members have demonstrated their commitment and willingness to step up to post 9/11 challenges. But we cannot shoulder the burden alone. We need and embrace a more comprehensive and more integrated partnership with our public sector colleagues. Security is not an option for the members of the American Chemistry Council.

Thank you for the opportunity to testify today. I am happy to answer any questions that you may have at this point.

The following information provides examples of security measures ACC members have long taken to protect their facilities, their employees, their products and their neighbors, and that are now being enhanced to reduce their vulnerability to terrorist attack. (On the advice of the FBI and the Department of Homeland Security, ACC will not release specifics about individual company security measures.) The vulnerability assessments conducted by ACC member companies -- and required by ACC's Responsible Care[®] Security Code -- have greatly assisted the review and enhancement of existing safety and security procedures.

Facility Security

Access Control

- Visitor sign-in logs & escorts
- Allow only authorized personnel to have physical access to key production units. Supervise any visitors.
- Close attention to access control at loading/unloading areas
- Install appropriate penetration-resistant doors and security hinges
- Install secure windows and doors with appropriate locks, including use of unbreakable plastics windows and window bars
- System of employee and contractor photo ID badges
- System for determining which cars, trucks, rail cars, marine vessels, and other vehicles may enter the site through which gates, docks, or other entrances, and under what conditions
- Electronic access control system that requires the use of key cards at main entrances and on other appropriate doors and that provides an audit trail of ingress and egress.
- CCTV system to monitor key areas of the facility
- System of parcel inspection (using magnetometers, x-ray screening, or explosives detectors).
- Require property passes for removal of property from the site.

Perimeter Protection

- Fences and exterior walls that make it difficult for intruders to enter the site
- Bollards and trenches that prevent vehicles from driving into the site at points other than official entrances.
- Vehicle gates with retractable barriers
- Personnel gates with turnstiles
- Setbacks and clear zones that eliminate hiding places near the site's perimeter, making it difficult for intruders to approach the site unnoticed
- Lighting that makes it easier for employees and even passersby to observe and possibly identify intruders.

Security Officers

- Develop a security center to better monitor and support security process
- Patrolling the site to look for intruders or irregularities
- Staffing site entrances to check ID's
- Maintaining entry and exit logs
- Handing out trucker safety lists
- Reminding employees and contractors of security policies
- Assisting in emergencies
- Written post orders to direct their activity

Backup Systems

- Electricity
- Communications (telephone & computer)
- Water, sewer, and gas
- Control centers
- Computer servers

Transportation Security

Marine

- Establishment of protocols for actions corresponding with different Homeland Security Threat and Marine Security (MARSEC) Levels.
- Visual inspections by company barge handlers of all incoming barges including walk arounds to look for suspicious items laying around or adhering to the barge sides, surface, etc.
- Visual inspections by the towing crew of product barges and voids.
- Harbor entry is observed by company personnel during the entire switching operation
- All individuals working on the barge docks must have company issued identification and be listed as being qualified for barge transfer operations.
- Additional cameras to monitor barges and the river front area.
- All contractors working in the facility must be on a list of approved contractors to enter the plant each day.
- All visitors must be accompanied by escorts to enter the facility.

Rail

- New fencing and gates so that rail cars are always within the plant perimeter.
- Procedural agreement with rail supplier that cars with hazardous materials are brought directly on site and spotted for immediate unloading. The cars are not left outside the plant perimeter.
- Joint policies and programs with railroads and trucking companies regarding the security of products during shipment, e.g., security communications, facility access, security in transit.

Truck

- Prior information on identity of delivery personnel and truck drivers entering a site.
- Requiring two forms of identification from truck drivers when entering the plant site.

- Using tamper evident seals, containers and container cages for product transportation.
- Conducting a vulnerability assessment of the company's value chain operations.
- Conducting security audits of appropriate truck terminals.
- Identifying secure locations for pre-loaded trailers.
- Communicating to truck companies requirements for en-route security
- Working with customers and carriers to reduce transit time of products, where appropriate.

Information & Cyber Security

Information Security

- Prohibit radio conversations about sensitive topics
- Alternatively use voice encryption for radio conversations
- Conduct the most sensitive conversations in person
- Prohibit employees from giving out potentially risky information over the phone, as one may not be sure to whom one is speaking.
- Shredding of old, outdated, or unnecessary copies of critical documents
- Lock file cabinets and trash bins
- Institute a clean desk policy
- Mark sensitive documents as "confidential".
- Provide employee training on document security practices

Computer, and Network

- Physically secure computer rooms, motor control centers, rack rooms, server rooms, telecommunications rooms, and control rooms, ideally with electronic or biometric access control systems that record ingress and egress.
- Employ firewalls, virus protection, encryption, user identification, and message and user authentication to protect both the main computer network and any subsidiary networks, such as access control systems, that are connected to it or to the outside.

- Training of employees to beware of ruses to obtain their computer passwords
- Require systems administrator to disable all Internet connection software that may be prepackaged in operating systems.
- Allow the principles of “least access”, “need to know,” and “separation of functions” guide the determination of user authorizations, rather than position or precedent.
- Remove signs indicating the location of the computing facility
- Equip the computer room with adequate communications capabilities to facilitate prompt reporting of emergencies
- Allow only authorized personnel to have physical access to central computer rooms. Supervise any visitors.
- Periodic analysis of transaction histories, looking for variances from the norm
- Periodic analysis of users authorizations, (unusual) timing, frequency, and length of access

Security Planning, Training, Drilling

- Enhance emergency response plans to include security component (e.g., add local law enforcement and FBI, procedures for evidence identification, collection & protection)
- Actions at elevated threat levels
- Participate in local area security network meetings, organizations, training and drills.
- Conducting emergency response drills that contain transportation security activities.
- Participate in local Security Alert Communications Network
- Training and drilling on:
 - Criteria and Thresholds for Identifying and Reporting Suspicious Behavior or Threats – Joint project of FBI and Chemical Sector ISAC
 - Activities Considered Suspicious in the Vicinity of Critical Sites
 - Security Activities & Responses at Differing Threat Levels
 - Response to Bomb Threat

- Identification & Response to Suspicious Mail
- Identification & Reporting of Suspicious Purchases and Inquiries –
Developed cooperatively between chemical industry and FBI
- Evacuation Planning Matrix – In conjunction with OSHA
- Possible Indicators of Al-Qaeda Surveillance – In conjunction with the
Department of Homeland Security
- Hazardous Materials Driver Anti-Terrorism Tips – In conjunction with the
Federal Motor Carrier Safety Administration
- CIO Cyberthreat Response & Reporting Guidelines – Joint project of CIO
Magazine, DHS, US Secret Service

Hiring and Employment Termination Practices

- Pre-employment screening to identify history of conviction for theft or violent crimes, of workplace violence or threatening behavior, or of interests inimical to the company
- Retrieval of worker's keys, access control card, and company ID
- Change combination locks and even some keyed locks
- Change or block computer passwords
- Escort departing worker out of the building to make sure he or she does not harm data, property, or people on the way out.

Performance: Security Code

	Tier 1	Tier 2	Tier 3	Tier 4
Assess Site Security Vulnerability	31 Dec 02 (100% completion)	30 Jun 03 (100% completion)	31 Dec 03 (100% completion)	31 Dec 03 (100% completion)
Implement Site Security Measures	31 Dec 03	30 Jun 04	31 Dec 04	31 Dec 04
Verify Physical Site Security Measures	31 Mar 04	30 Sep 04	31 Dec 05	***

*** Tier 4 facilities will have no offsite consequences and will not require verification

Mr. MURPHY. Ms. Gibson.

Ms. GIBSON. Good afternoon, Mr. Chairman and members of the subcommittee. My name is Jennifer Gibson and I am the vice president of government and public affairs at the National Association of Chemical Distributors.

NACD's 300 member companies represent between 80 and 90 percent of the chemical distribution facilities in the United States. NACD members process, repackage, warehouse, transport and market chemical products for an industrial customer base of 750,000. Approximately 18 billion of U.S. chemical industry sales are through distributors.

To become and remain a member of NACD chemical distribution, companies must take title to product and adhere to management practices related to health, safety, security and the environment as outlined in the association's Responsible Distribution Process [RDP].

Since well before September 11, 2001 NACD members have adhered to the policies and procedures outlined by the Responsible Distribution Process. These requirements have always called for security and risk management considerations within and outside each facility. Members are also required to complete two stages of independent third-party verification of their RDP policies and procedures including an onsite independent verification once every 3 years. Companies who are found to be out of compliance by the third-party verifier are terminated from NACD membership; therefore, security is not a new issue for chemical distributors.

NACD as the leading association of chemical distributors was the first industry association to adopt new additional practices addressing security following September 11. In April 2002 NACD added security requirements to RDP within key distribution operations, specifically in the handling and storage of chemical products at facilities, in carrier selection for distributing chemical products and in customer qualifications for chemical products of concern to various Federal agencies. NACD's RDP verification is now underway to confirm implementation of these new security requirements at sites and we expect all of these verifications to be complete by the end of next year.

Regarding the current Federal programs addressing security at chemical facilities, we think the Federal Government has gotten off to a very good start. NACD also supports Federal legislation that would mandate vulnerability assessments for chemical facilities and recognize the management practices already in place that provide for enhanced security of chemical manufacturing and distribution.

We would also like to see DHS develop a vulnerability assessment model for chemical distribution facilities, as it did for the chemical manufacturing sector. We have five programs underway to close potential loopholes that could allow commercial HAZMAT transport drivers with felony records to obtain positions at chemical distribution facilities unbeknownst to their employers. The plan is to fingerprint all commercial driver's license holders with HAZMAT endorsements is a positive step. We strongly encourage the subcommittee to urge TSA and DHS to utilize the successful fingerprinting program already in place for airport and aviation

personnel. The hazardous materials truck driver population is more than double the size of the aviation personnel that require fingerprinting. We urge the subcommittee to insist that Congress and the executive branch consult with the American Association of Airport Executives that designed, implemented and operated the aviation clearinghouse to ensure that there will be no interruptions to the interstate transportation of chemicals because of the inability to process HAZMAT driver fingerprints. This program was originally scheduled to go into effect late last year and now the effective date will be April 1st of this year.

In the event of a catastrophic occurrence at a chemical distribution facility, Federal agencies should work collaboratively with first responders, industry and incident response agencies. It is important that Federal agencies work side by side with as many stakeholders as necessary to respond to any catastrophic event should it occur. Existing emergency response networks that are well-established and widely used by industry, namely CHEMTREC, play a vital role in crisis and incident management.

Third, the only shortcoming we perceived in the area of Federal support of local and State emergency response activities is a lack of regular communication in some cases and, therefore, the possibility of uncoordinated activities. The Federal Government should continue to take a leadership position in directing more formalized and regular communication among federally supported local and State emergency response personnel as well as individuals with similar responsibilities at chemical facilities. We greatly applaud the government's development of the Information Sharing and Analysis Centers that includes the chemical sector as one of several with which it collaborates and shares information on related security issues.

Thank you for the opportunity to address the subcommittee today. I will be happy to answer any questions.

Mr. MURPHY. Thank you.

[The prepared statement of Ms. Gibson follows.]

Exhibit **8**
Witness *J. Gibson*
Date *2-23-04* Rpt. *JJA*
**Powers
Garrison &
Hughes**

**WRITTEN TESTIMONY OF THE
NATIONAL ASSOCIATION OF CHEMICAL DISTRIBUTORS
ON THE HEARING OF THE
HOUSE SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS
TITLED "COMBATING TERRORISM:
CHEMICAL PLANT SECURITY"**

**February 23, 2004
Moon Township, Pennsylvania**

INTRODUCTION

The National Association of Chemical Distributors (NACD) is an international trade association headquartered in Arlington, Virginia. NACD represents 300 chemical distribution companies in the United States and Canada. These companies are believed to represent between 80 and 90% of the chemical distribution facilities in the nation and more than 90% of the industry's gross revenue.

NACD member companies process, formulate, blend, re-package, warehouse, transport, and market chemical products exclusively for an industrial customer base of approximately 750,000. Approximately \$18 billion of U.S. chemical industry sales are through chemical distributors, who are also actively engaged in various phases of import/export trade. Chemical distributors' industrial customers use these materials to produce such everyday items as computers, detergents, cosmetics and toiletries, food flavorings, perfumes, automobile parts, water purifiers, fiberglass, plastics, pharmaceuticals, paints and coatings, and many other products.

To become a member of NACD, chemical distribution companies must take title to product and adhere to management practices related to health, safety, security, and the environment outlined in the Association's industry practice known as the Responsible Distribution ProcessSM (RDP).

Before a company is admitted as a member, it must first be approved by successfully completing an independent, third-party verification of its written policies and procedures under RDP. To ensure continued compliance with RDP, every member must undergo an on-site verification by an independent third-party verifier once every three years. This mandatory practice has been in place since 1998 and members are currently undergoing their second on-site verification which will be completed at the end of 2005. NACD's Responsible Distribution ProcessSM is the most comprehensive and rigorous industry practice of any in the chemical industry primarily because of its requirement for independent third-party verification.

Although chemical distribution is a sector of the chemical industry, distribution facilities differ in numerous ways from chemical manufacturing facilities. One notable example is the release of toxic emissions from everyday operations. According to data compiled each year by the Environmental Protection Agency (EPA), chemical distribution is a minor source of environmental releases. Of all industrial sectors required to submit annual toxic release reports, including the chemical industry, chemical distribution is by far the lowest emitter of toxic emissions. The average yearly release per distribution facility is just over 3,000

pounds over a 12-month period. While the possibility of chemical releases exists at chemical distribution facilities, it is minimized because of several factors, not the least of which is adherence to the industry's environmental, health, safety, and security practice—Responsible Distribution ProcessSM—among NACD members.

Chemical distribution is also a safe industry in which to work. Industry data show that chemical distribution is a safe industry in terms of employee injuries and fatalities at NACD member companies as well as in transportation-related incidents. For example, last year among 18,150 workers employed by NACD member companies, there were 619 OSHA-reportable employee injuries that occurred within distribution facilities, down by 137 injuries the year before, and one fatality. Among transportation-related incidents, there were 28 injuries among member companies and two fatalities.

**WRITTEN TESTIMONY OF THE
NATIONAL ASSOCIATION OF CHEMICAL DISTRIBUTORS
AT A HEARING BY THE HOUSE SUBCOMMITTEE ON NATIONAL
SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS**

My name is Jennifer Gibson and I am the Vice President of Government and Public Affairs of the National Association of Chemical Distributors (NACD). I am pleased to have the opportunity to appear before you today to address the state of security within the chemical distribution industry.

Security Has Always Been and Continues to Be a Focus

Before I address the three specific questions the subcommittee has posed to participants in today's hearing, let me begin by stating that security has always been a focus at chemical distribution facilities. Any facility that handles hazardous materials understands that their products have the potential to impact its employees, the local community, and the environment. Most chemical facilities are regulated by multiple federal, state, and local agencies, some of which have required security and risk management provisions for years. Mishandling our products means loss of revenue in an industry in which margins are very low and where the competition is very high.

Additionally, prior to September 11, 2001, NACD members adhered to policies and procedures outlined by the Association's Responsible Distribution ProcessSM (RDP), an industry practice that has been in place since 1991. Compliance with RDP is a condition of membership in NACD. These requirements have called for security and risk management considerations within and outside the distribution facility for the past thirteen years. However, our member companies go beyond simply adhering to a code of management practice. They are also required to complete two stages of independent, third-party verification of these policies and procedures, including an on-site third-party verification once every three years. Since 1998 when NACD began requiring on-site third-party audits, twenty companies have been found to be out of compliance with RDP and have subsequently been terminated from membership. Therefore, security is not a new issue for chemical distributors. It is a consideration that is a part of the industry every day.

NACD, as the leading association of chemical distributors, was the first chemical industry association to adopt new additional industry practices that address security following 9/11. In April 2002, NACD added security requirements to RDP within key distribution operations, specifically handling and storage of chemical products at facilities, carrier selection for distributing chemical products, and customer

qualification for chemical products of concern to various federal agencies. NACD's existing on-site, third-party verification requirement is currently being conducted to verify implementation of these new requirements at distribution sites. To date, 55 facilities have been verified with an additional 70 on schedule through 2004 and the remaining 175 to be verified before December 31, 2005.

On-site, third-party verifications at distribution companies with multiple facilities are randomly-selected from among the company's locations. The purpose of the random selection is primarily to assure that the company has successfully implemented RDP policies and procedures at all sites, not just company headquarters, which were verified in the first three-year cycle, 1999-2002.

If a company is found to be out of compliance by the verifier, the company has a maximum of twelve months to demonstrate it has rectified the findings of non-compliance through a second, full verification at the facility. If in the second verification the company fails again, it is terminated from membership. In some cases, a company can fail and be terminated from membership on the first verification if non-compliance of RDP requirements is systemic throughout the facility.

GAO's Report, *Homeland Security: Voluntary Initiatives Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown, Did Not Cite Chemical Distribution as a Security Vulnerability.*

The General Accounting Office intentionally excluded chemical distribution from among the sectors of the chemical industry where additional security measures must be focused. To paraphrase a conversation we had with GAO's Peg Reese, who was a contact for the report, the GAO was aware of chemical distribution as a sector of the chemical industry, but, through its conversations with EPA and others, it concluded that distribution facilities are not high-risk facilities. Nevertheless, under RDP, NACD members continuously consider ways to enhance security.

NACD is working closely with FBI, DHS, other association partners through intelligence sharing and constant collaboration.

NACD is now and has been since September 2001 actively engaged with senior officials within the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) regarding chemical distribution security. NACD and its members have met with FBI and DHS officials on numerous occasions over the past two years. We remain engaged and stand willing to support reasonable federal actions that achieve further security of distribution facilities.

I would now like to address the specific questions posed by the Subcommittee.

1. Generally speaking, we regard the current federal programs addressing security at chemical facilities as a good start. Specifically, NACD supports federal legislation that would mandate vulnerability assessments for chemical facilities and recognize the management practices already in place that provide for enhanced security of chemical manufacturing and distribution. However, we would like to see DHS develop a vulnerability assessment model for chemical distribution facilities as it did for the chemical manufacturing sector. While not specifically facility-related, the following statements address an integral part of the safe and secure storage and distribution of chemicals. We applaud programs underway to further close potential loopholes in the ability of commercial HazMat transport drivers who have committed felonies in the past to occupy truck driver positions at chemical distribution facilities unbeknownst to their employers. The plan to fingerprint all CDL holders with HazMat endorsements starting on April 1 is another positive step. We would strongly encourage the Subcommittee however, to encourage TSA and DHS to utilize the successful program of advance planning, preparation and implementation of fingerprinting used for all airport and aviation personnel occupying those facilities. That operation worked smoothly, efficiently and without complaints that these personnel were being unduly charged. The hazardous materials truck driver population is more than double the size of the aviation personnel that required fingerprinting. We again strongly encourage this Subcommittee to insist that Congress and the Executive Branch consult with the American Association of Airport Executives that designed, implemented and operated the aviation fingerprinting clearinghouse, to ensure that there will be no interruptions to the interstate transportation of chemicals because of the inability to process hazardous materials driver fingerprints. Fingerprinting of these drivers, originally scheduled to begin on November 1, 2003, is now scheduled to begin on April 1, 2004.
2. In the Event of a Catastrophic Event at a Chemical Distribution Facility, Federal Agencies Should Work Collaboratively with First Responders, Industry, and Incident Response Agencies. It is important that federal agencies work side-by-side with as many stakeholders as necessary to respond to any catastrophic event should it occur. Existing emergency response networks that are well-established and widely used by industry, namely CHEMTREC, play a vital role in crisis and incident management.
3. The only shortcoming we perceive in the area of federal support of local and state emergency response activities is a lack of regular communication and,

therefore, the ever-present possibility of uncoordinated activity. The federal government should take a leadership position in directing more formalized and regular communication among federally supported local and state emergency response personnel as well as individuals with similar responsibilities at chemical facilities. We greatly applaud the government's development of the Information Sharing and Analysis Center (ISAC) that includes the chemical sector as one of several with which it collaborates and shares information on related security issues.

Thank you for the opportunity to address the Subcommittee today. I would be happy to address any questions you have.

Mr. MURPHY. I want to thank all the witnesses.

Mr. Stephenson, I'd like to start off with a question for you. In your report you write on page 6 of it, it says, "In testimony on February 6, 2002 the Director of the Central Intelligence Agency warned of the potential for an attack by al Qaeda on chemical facilities."

Without getting too much into intelligence on that, what actions have been taken, voluntary actions from the chemical industry? In your analysis are we at the same risk, elevated risk, or low risk based upon some of the actions we have heard today?

Mr. STEPHENSON. Unfortunately, we haven't done any updates to our work in the last year, but voluntary actions by industry have gone a long way toward reducing the risk, I would say.

Unfortunately, organizations like ACC only represent a small portion of the facilities that store or use hazardous chemicals. In addition, we at GAO are satisfied that there is still no Federal requirements that mandates vulnerability assessments across the board to all facilities who use hazardous chemicals.

Mr. MURPHY. Let me followup with that so that I understand the association. The American Chemistry Council did an assessment of 15,000 facilities.

Mr. Durbin. That's correct.

Mr. MURPHY. Now, I list some of the other associations, the National Association of Chemical Distributors, and then there are manufacturing associations, but according to the American Institute of Chemical Engineers, American Petroleum Institute, State association, etc., when you add all these associations together, two things: one, how close are we to having all 15,000 plants and distributors involved in this; and, two, do all these associations adhere to the same security guidelines identified by the ACC?

Mr. DURBIN. I will try to answer that. If you look at the population of the 15,000 communities, you know, again, ACC or chemical manufacturing is only about 7 percent, you add the others that you mentioned, you certainly do start to add up—add to that number. However, if you look at the vast numbers, the larger numbers, you're looking at water treatment and drinking water facilities, agriculture retailer facilities, refrigeration warehouses that use ammonia for their refrigeration.

So, again, you're still not—even if you mention all the—take all the ones you mentioned, you're not coming close to getting to the majority of facilities that would fall under that 15,000.

Mr. MURPHY. Now, how much has been—in terms of the compliance issues, do we know how much money has been invested so far and what will it take for all the plants to be in compliance with just the standards that you have said? Any idea what we're talking about?

Mr. DURBIN. Again, just speaking for the ACC members, we don't have a definite number yet, we're actually doing some economic surveys with the membership. And I will just qualify that over the last year the investments are now being made.

What I can tell you and what we do know is that the number at this point is literally over \$100 million and into the hundreds of millions of dollars that have been invested. Again, on average right now it appears that there has been at least \$2 million per

company that has been spent. You know, membership of 140 companies, you're ranging in size from very large to very small; but, again, we are talking literally over hundreds of millions of dollars that have been spent already.

Mr. MURPHY. And, Ms. Gibson, I think in your testimony regarding the National Association of Chemical Distributors, I think you mentioned that plants or distributors have been given a couple chances to comply.

Ms. GIBSON. Right.

Mr. MURPHY. By the third time, third strike they're out.

What enforcement abilities do you have on a national level or State level with regard to if plants and distributors do not reach their security guidelines that you have set on a voluntary basis, what can you do besides kick them out of the association?

Ms. GIBSON. That's our measure that we can take to get them to comply, and if they don't, well, they're out. And that's why we support Federal measures to require these measures.

Mr. MURPHY. Are there such things as the association working, for example, that those who may purchase products made by these plants or distributed by the distributors that—to discourage people from purchasing from plants that are not in compliance? That's a big financial aspect added to it.

Ms. GIBSON. Right. Exactly. Yeah, to be a member of NACD everyone has their NACD logo, Responsible Submission Process logo, and purchasers know that these products have gone through Responsible Submission Process, so that is a good economic incentive.

Mr. MURPHY. So, for example, if your company is distributing chemicals manufactured by other associations going through the States, does word go out that XYZ Co. is not in compliance, and therefore other plants and distributors are given some sort of warning not to purchase from them? Does it go that far?

Mr. DURBIN. If I may, I'm not an attorney, but I believe you start to get into problems of antitrust concerns if you have members of an association starting to single out a particular company for any reason to say do or do not purchase from that company.

Mr. MURPHY. So then this just goes—

Ms. Witmer, do you want to add something to that?

Ms. WITMER. I was just going to follow that up that we, in fact, follow very strict antitrust rules and that whenever there's a gathering of association members, our legal counsel reminds them, you know, that they are not, in fact, to talk about those kinds of activities for, you know, fear that we would be in violation of the antitrust.

And that is why, as Ms. Gibson pointed out, we are so strongly in favor of Federal legislation, so that there is one national standard and then perhaps maybe a reporting mechanism as well.

Mr. MURPHY. So the bottom line, in absence of Federal standards requiring this, there's no enforcement capability that any of your associations can foster, even within your association, other than kicking them out?

Ms. WITMER. Not from a legal perspective.

Ms. GIBSON. Right.

Mr. MURPHY. Let me ask you another thing, too. How long before the highest-risk facilities are brought up to a standard that your

agencies have set? Are we at that level yet, the highest-risk facilities?

Mr. DURBIN. Again, speaking for the ACC facilities, they were broken into four tiers; the tier I facilities completed their vulnerability assessments at the end of 2002, by the end of 2003 they would have had to implement all their security enhancements.

Now, they have until March of this year to have those verified, but those tier 1 facilities are, again, essentially done; tier 2 facilities will be done by June of this year and all of our facilities are, again, as I mentioned in my testimony, are scheduled to be through by the end of this calendar year.

Mr. MURPHY. One of the recommendations I had for security here, is it possible within the plants and distributors, large or small, that some external source could hack into the computer and cause problems with regard to release of chemicals or locking security measures, or is it all done internal with no connection to the outside?

Ms. GIBSON. I'll let Mr. Durbin speak to this as well, but I know that's been—specifically in the past several months now that we've kind of addressed the facility perimeter security, we've really started to look more at the cyber security aspect of it, really evaluating what information those companies have on their computers and how can that information be protected, because that is just as important as the physical security.

So we're starting to get into that more and more and there's a joint industry group looking at those in collaboration with the government.

Mr. DURBIN. And, in fact, I would say what's interesting about the cyber security piece of this is that more than the physical security side, they almost have a leg up, because many of our member companies have already been working very closely on cyber-related issues because of simple E business, business-to-business issues, Y2k issues.

So there were already groups of our member companies very much focused on securing not only their IT systems and information, but, again, many of our facilities and our processes are controlled by computer, so making sure that they cannot be hacked into from outside, outside the facility, to be able to cause a release.

Mr. MURPHY. And then one area, too, I want to ask about because the plants that we specifically have heard about today, a couple of those were investigated by the media, and we know there's many more throughout the country they covered; for example, in the 60 Minutes story, Baltimore, California, New York, other places, too.

Despite what we heard earlier today on Univar, despite efforts taken on those sites, they still cannot block access through the rail lines that bisect their plants and I saw mention in here that the rail industry and chemical industry are working cooperatively.

What else do we have to do on those sites other than—I don't know, what else can be done on those sites, because that still seems to be a critical aspect, materials transported by rail, by truck; where do we go from there?

Mr. DURBIN. No question; and I think, as Ms. Witmer mentioned in her testimony, we did establish a task force between AAR, the

Rail Trade Association, and ACC to address three specific issues. One was communication to our customers, and I can discuss that more in a moment, but the two other areas were storage in transit and access to the plants.

Traditionally, you know, the railroads and transportation of our chemicals, obviously a very important part of your business, intended to have fairly free access to the facility, you know, 24 hours a day drop-off materials and what have you.

A lot more has gone into now determining, kind of putting together rules of the road for access to the facility, gates over the rail access, and in some cases where there aren't gates you've still got electronic surveillance and alarms and other things that are now instituted. But, again, this is an evolving process and one where we're continuing to find the existing vulnerabilities and working very hard, very fast, to try to address those vulnerabilities.

Mr. MURPHY. Also, I know that I have little doubt that some reporters, all they have to do is walk on those plant sites and look at those aspects and, as was already testified to, there are reporters sent by the media to see what is actually happening there. And I don't want to see these kind of breaches take place without a quick response. I really need you to know that, and I appreciate that you will continue to work with Congress in order to draft these high-standard initiatives to make sure we protect these areas for the public.

Mr. Turner.

Mr. TURNER. Mr. Chairman, when we talked with our first panel about the issue of EPA and the Department of Homeland Security being the lead agency with respect to having authority in this terrorist threat arena, we all voted for the Department of Homeland Security.

I want to give each of you an opportunity to tell us your preference: the Department of Homeland Security or EPA and your rationale.

Mr. STEPHENSON. Well, I don't want to give you my preference. I will say that EPA has a great deal of knowledge on this subject stemming from its Clean Air Act responsibilities and the 1990 amendment which established this risk management plan approach, so they have an incredible amount of knowledge on those 15,000 facilities with hazardous chemicals.

On the other hand, Department of Homeland Security brings to it the threat-based analysis. Both of those things have to be considered when you're assessing vulnerabilities at an individual facility.

So I would hope that they're working very closely together. I think both of them have a contributing role in this. DHS, since it is a security issue, may be more appropriate. But I would hope that all this experience that EPA has developed over the last decade won't go to waste.

Mr. TURNER. Ms. Witmer.

Ms. WITMER. The Pennsylvania Chemistry Industry Council supports DHS as the oversight agency for security, presumably because they have the expertise in developing and assessing security plans.

There is potentially a role for EPA to play, certainly from a response perspective. Their mission is to protect the environment, not to—they don't have the expertise to assess the security plans.

Mr. DURBIN. ACC has also been on record that DHS would be the appropriate primary agency to have a lead over the chemical sector security, but, again, that is not to say that there isn't a need to be able to pull in the expertise of other agencies.

No. 1, I would point out that while we have worked and will continue to work very closely with EPA on all of their programs what is needed now is an agency that not only has the charter mission to protect all the critical infrastructures, but they can appropriately look across all of the interdependencies of the various critical infrastructures. If you look at any one facility you've got, you know, the power grid coming in, water grid, transportation grid, and you need to be able to coordinate all of those.

Additionally, if I can add a little bit more context as well, you're talking about an industry that already has a long history of working with various Federal agencies not just on physical hardening of our facilities but on the potential misuse of our products, whether they're stolen or have chemical weapons conventions, dual-use chemicals, drug precursors, and even the fertilizer industry was mentioned earlier that works with ATF. And there's a coordination that needs to go on here that involves EPA, Department of Commerce, Department of State, ATF, the FBI, and I think that the way DHS has been created it's only appropriate that they have to play that primary coordinating role.

Ms. GIBSON. I would concur with Mr. Durbin's comments about I think the most important aspect is to have one clear agency coordinating all these security efforts. And given the focus of DHS—threat, security analysis assessment, vulnerability assessment, site security approval—I think they are the most appropriate agency to take on that role.

Mr. TURNER. My next question goes to the association of representatives. I already indicated in panel one that I'm a fan of the EPA processes that require disclosure of information because of how it has assisted the community in empowering them to be able to be at the table and have an impact, I think even to the benefit of affecting the facilities by giving them additional security consulting information, even though at times I think it has been an augmentation of the government's ability to advise and to plan for potential incidences at these facilities.

For your members, though, what are their thoughts with respect to the extent of the public information that is available? Are they concerned as it relates to a terrorist impact that so much information is currently available about them?

Ms. WITMER. Members of the Pennsylvania Chemical Industry Council are urged to work with their communities, including their residents in the area in which the facility is located, as well as the first responders and government officials to reach out and let them know what is happening at the facility.

As far as an actual security plan, no, we don't think that individuals in the neighborhood, so to speak, should, in fact, be able to look at those. The emergency management plans are available to the local first responders. They have them, they know what's there

at the facility, so that if there is an incident, when they respond they know what they're dealing with.

So there's a balancing act that we think we are successfully negotiating. We don't think there needs to be that information placed on the Internet for anyone to look at, but there does need to be a lot of communication with the community in which the facility is located.

Mr. DURBIN. I would concur with Ms. Witmer's comments. There is information that has to be shared with the community and then there's talking about the security vulnerability assessments and the plans we've implemented to address those vulnerabilities and making them publicly available.

Ms. GIBSON. Part of NACD's Responsible Distribution Practice for companies is to become involved with the local agencies and invite them for tours and go through the training and emergency response exercises, so we clearly support as much communication as possible with the local officials.

As far as having information on the Internet, that's—everybody knows the obvious dangers of that—that could easily fall into the wrong hands. So, as Ms. Witmer said, it is a balancing act.

Mr. TURNER. My next issue relates to as individual plants in several communities begin to take efforts to secure their facilities, they are learning more than they did before in the capture of this information, the sharing of this information, so that our collective learning curve can be diminished, and then we can adopt best practices as it occurs.

From the association's perspective, you talk about your efforts to capture that expertise and disseminate it among your members and also from GAO's perspective the lost opportunities.

And I'll go to Ms. Gibson.

Ms. GIBSON. I'm sorry, I don't quite understand the question.

Mr. TURNER. Your members are undertaking security enhancements.

Ms. GIBSON. Yes.

Mr. TURNER. And they may be undertaking very different types of security enhancements that they might benefit from sharing that information among each other.

Ms. GIBSON. Right.

Mr. TURNER. Can you tell us what among your association you're doing to help capture that information and share it among the various members so that we can all have a greater enhancement of that?

Ms. GIBSON. Kind of within the association it's always—security is a funny topic, as you know; companies are sometimes reluctant to actually publicize the specific measures they're taking. But we do have guidelines under the Responsible Distribution Process for companies to follow and they have done that.

We're also probably going to start this year outlining some best practices along the RDP process to go over at our annual meetings so those companies know all the different areas and programs to share information and what works.

Mr. TURNER. Obviously the reason why I'm asking the question is I don't believe we're doing very well. I know you've indicated some effort to do that, but still this is, you know, a critical area

where we really need to be finding our best and brightest and best solutions and sharing them.

Mr. GIBSON. Even among—just among all the different chemical trade associations, there is a lot of communication among all the different trades; even though distribution may differ from manufacturing, we work very closely together on these issues through the ISACs and different initiatives.

Mr. DURBIN. Just to follow that, many of the guidelines we put together were in conjunction with NACD and others so we try to reach out there. As far as—I think you put your finger on a very important role and something that we do need to be able to capture, the best practice, and make sure that we share this appropriately.

Again, just within our association and among the association, issues around process safety or just safety has always been an area where we've kept very robust networks of sharing, sharing best practices.

We are now doing the same thing on the security level. We have a security network. In fact, just last week in Washington we had a 2-day meeting, which we had about 40 security directors from facilities around the country, and it is structured in such a way just to put the issues on the table that they are having issues with, concerns, or, again, best practices, what are you guys doing about this. And so in that regard we're seeing a very robust communication with our members.

I think we do need to look at how do we capture that and make sure we get it out, you know, more broadly. All of the guidelines that we've put together, even our Responsible Care Security Code, is not something we keep insulated just to ourselves; it's public, it's published, available to anyone out there who wants to use those guidelines.

Ms. WITMER. Would you like me to address that or do you want to go on? It's really just an agreement statement with, you know, the other two responders.

One thing that we do differently perhaps at PCIC, we have an Internet-based ability for folks in the security network to talk to each other if they have a particular issue that they're dealing with. Rather than having to come in physically to a meeting to talk about it, we have set up two-way communication on the Internet where they can discuss those sorts of issues as well.

Mr. TURNER. Mr. Stephenson.

Mr. STEPHENSON. Just quickly, the Information Sharing and Coordination Centers [ISACs], that were set up for each of the 13 infrastructure elements are designed for this purpose, to share best practices. These are public/private partnerships consisting of the lead trade association and these Federal agencies responsible for a given infrastructure.

So maybe there's a little bit of confusion since DHS is new to this responsibility, and coordination that isn't working as well as it should. DHS is taking charge of vulnerability assessments, but has not fully addressed the information sharing aspects of the ISAC function. So I think hopefully the Federal Government can encourage better sharing of information as well; it's a role we need to fulfill.

Mr. MURPHY. Anything else? Mr. Turner.

Mr. TURNER. I'm finished.

Mr. MURPHY. Mr. Shays.

Mr. SHAYS. Thank you. I'd like to have a sense of who handled security before there was a terrorist threat. Who had the responsibility.

Mr. DURBIN. I'm sorry. Within the government? Within industry.

Mr. SHAYS. Walk me through it.

Mr. DURBIN. Well, again, security I think before September 11th was certainly—it was dealt with at the company level, certainly from a different paradigm, at least here in the United States.

I can tell you some of our larger corporations that are, you know, multinational depending on where they're located, certainly have had to deal with the issue of terrorism, whether it's in Ireland or different parts of Africa or Indonesia or what have you. But I think prior to September 11th, our security directors at our companies were dealing more with the traditional break-ins, misuse of chemicals, and even just employee issues within the facilities.

Mr. SHAYS. So the EPA—was EPA the—

Mr. DURBIN. No, there was no specific government role over security of chemicals.

Mr. SHAYS. So they dealt with safety, they didn't deal in any way of maybe having a fence up or something like that? EPA wouldn't require that.

Mr. DURBIN. Not that it would have been required. It would have been part of the risk management plans that the EPA program encouraged and helped develop to get the communication going from the facility, the plant community and the local responders. I mean, that discussion was then able to say what is necessary—

Mr. SHAYS. But it happened under the context of the EPA.

Ms. WITMER. It was more of safety, you know—as you know, a lot of these facilities are on rail lines or in a community where there are kids walking and so, you know, it was a safety issue.

Mr. SHAYS. So it was a security issue, but not from the standpoint of people intending bad things, but still security was handled by EPA in that sense; correct.

Ms. WITMER. I would disagree that it was security, but that it was more of safety.

Mr. STEPHENSON. The risk management plan was premised on accidental releases, not intentional releases, but, again, they did worst-case scenarios on an accidental release and that's where the information on putting millions at risk in certain situations came from. Chemical facilities themselves came up with those worst-case scenarios, it wasn't EPA.

Mr. SHAYS. So basically it was silent to security—basically the EPA and security was—and the consequence of a release was whose responsibility? OSHA's.

Mr. STEPHENSON. Well, OSHA set safety standards. Consequences of a release is part of what the risk management plans were supposed to address. Again, that's where the risk numbers came from.

And let me correct something on the earlier panel, it wasn't—the chemical companies—and ACC can correct me if I'm wrong—did look at things like wind direction, types of chemicals used, and

proximity to populated areas. This notion of a 360-degree pattern isn't exactly right from my understanding of what the risk management plans did and what the worst-case scenario estimates involved.

And also the one gentleman was right. The worst-case scenario was from a single vat, whatever the largest toxic chemical that was stored onsite. So your question about could a terrorist act be worse; yes, if for example it targeted two vats, it would be worse than one.

Mr. SHAYS. I felt that it was such a simple question, that it wasn't a trick question. All he had to do was say yes, it would obviously be worse if there would be more.

But the bottom line is the worst-case scenario under the EPA makes certain assumptions.

Mr. STEPHENSON. Right.

Mr. SHAYS. And one of those assumptions was that it was going to be, as you said, one vat.

Mr. STEPHENSON. Right.

Mr. SHAYS. You could have a whole host of them, correct, under a terrorist attack.

Mr. STEPHENSON. You could. You could. And the difference between the 4,000 number that the Department of Homeland Security quoted and the 7,000 from the risk management plans isn't exactly clear.

Mr. SHAYS. Currently what.

Mr. STEPHENSON. DHS mentioned 4,000 high-risk facilities and if you look at the risk management plans it has about 7,000 facilities affecting over 1,000 people, so I'm not sure what the 3,000 difference is.

You can get part way from the 15,000 facilities by eliminating the ones that affect under 1,000 population. That's a good share of the 11,000 number. But then DHS said there were 4,000 facilities that affect 1,000 or more; the risk management plans say there are 7,000 facilities that affect 1,000 or more. So I'm not clear what that 3,000 difference is.

Have I thoroughly confused you?

Mr. SHAYS. No. I mean, I was confused by the comments earlier. I find that we try to understate the concern to not get people anxious, and in the process there's not—I don't have a constituent right now who really believes there is a terrorist threat. Well, I am overstating. We've minimized it to such an extent.

I mean, I wrote down while you were testifying, I wrote down that basically I don't feel people really believe there's a threat. And if they did believe there was a threat, they think the odds are so low that it will impact them that they're not concerned.

And I don't feel any, you know, what's said in rooms in Washington are the chemicals are the greatest vulnerability, they represent the potential greatest harm, that they are the most tempting target, that their security is not all that great yet, and we know that and from those who would intend to do harm, you know. But it's kind of like someone who swims in shark-infested waters. They get out and say, listen, I did it, there's no big problem here. But there were still sharks there and you were fortunate you didn't get caught up in it.

I guess my point to all of you is that I'm just fascinated to know when there is an attack on a chemical plant, what the industry is going to say. I just don't know what they're going to say, because we all know right now we're very vulnerable. That's the reality. We are extraordinarily vulnerable.

Mr. DURBIN. If I could, Mr. Shays, that's exactly why an organization like the American Chemistry Council said we think we've gone out and we're doing the right thing. Our members have set very vigorous guidelines for themselves and they're meeting their own deadlines. But we know it's not enough. We know we don't represent the entire community of concerned facilities, facilities that would be of concern, and why we think that there does need to be Federal legislation that would establish guidelines for everyone. We have been actively trying to get legislation enacted and would be happy to work with you.

Mr. SHAYS. Let me ask you this: Do you do plume studies for these various plants? Do you recommend that they do that? Was it being done under EPA?

Let me back up a second. I still don't know who deals with consequence. That's what I don't understand. Before there was the concern of terrorism, who dealt with consequence?

Mr. DURBIN. Meaning if an incident were to occur?

Mr. SHAYS. Yes, an accident.

Mr. DURBIN. Well, that's something that the risk management plans help to coordinate what would be the response at the local level. I mean, I think what's clear to say no matter where—

Mr. SHAYS. I guess I don't have a sense of the sophistication of the consequence management. Does it vary from State to State, community to community.

Ms. WITMER. If there's an incident in Pennsylvania, if there is an accidental release in a facility or if there's a distribution—

Mr. SHAYS. This talks to pre-September 11th.

Ms. WITMER. Right. Exactly.

If there was an incident involving hazardous material the primary State agency would be the Department of Environmental Protection because they're responding to the incident from a cleanup—a consequence—a cleanup perspective, as well as, you know, the local first responders being the first ones on—I think that's what you're getting at as the consequence.

Mr. SHAYS. That's part of it. Were there pre-September 11th automatic procedures that so many homes within a certain area have to be evacuated and so on.

Ms. WITMER. It depends, you know, if it was a transportation-related incident or if it was at a facility, as well as, you know, what the material was that was involved. And that was part of the risk management plan that was developed by the facility.

Mr. SHAYS. So if it was a certain material there were just instantly guidelines that would—and were local communities apprised of those.

Ms. WITMER. Absolutely. A material safety data sheet for each of the chemicals is provided to the local communities.

Mr. STEPHENSON. That's one of the primary purposes of the risk management plan is so that the first responders know what's going

on in that chemical plant and know what could potentially happen if there was an accidental release.

Mr. SHAYS. And that was under the auspices of the EPA.

Mr. STEPHENSON. Right. It existed for over a decade.

Mr. SHAYS. So what happens now if there is a terrorist attack? Is EPA in the ball game.

Ms. WITMER. From—I think we're talking about—

Mr. SHAYS. I'm talking consequence now.

Ms. WITMER. Right. Exactly. So we're talking after the incident.

Mr. SHAYS. Yes.

Ms. WITMER. And, of course, the EPA would have a role. And I think what each of us said is that EPA does have a role and that it's from a consequence perspective but not from before the incident, from determining what the vulnerability is and from setting guidelines and standards on what is appropriate from a security standpoint. EPA, from my perspective with the Pennsylvania Chemical Industry Council, would come in from a consequence management role.

Mr. SHAYS. Wouldn't their role be far more important than DHS to deal with the consequences? What does DHS know and why would we reinvent the wheel? I mean, who cares.

I mean, you know, if a building is on fire the fire department comes out and puts the dang thing out. And whether or not it was, you know, an arson or a natural cause, we deal with it the same way. That's kind of what I'm wrestling with right now.

Mr. STEPHENSON. Well, EPA does have an emergency response capability to handle such things as the hazardous spill in the Baltimore Tunnel that happened less than a year ago, or anthrax in the Capitol Complex, as you know.

However, I think the ACC witness said it best. There's some cross-agency issues here that all need to be coordinated. Transportation used to be Department of Transportation, now it's Homeland Security. So there's a coordination function.

Mr. SHAYS. They moved that section over; correct.

Mr. STEPHENSON. Right.

Mr. SHAYS. We're not talking about that. They didn't move EPA into, you know, DHS.

Mr. STEPHENSON. Right.

Mr. SHAYS. It's still EPA.

Ms. WITMER. That's why I think we need an agency to be the oversight and coordinating agency because you have that many different agencies that have a role, but you need someone to be able to be the director.

Mr. SHAYS. And who should that be.

Ms. WITMER. Department of Homeland Security.

Mr. SHAYS. Why, if it's consequence.

Ms. WITMER. But there's more than consequence involved in first hopefully preventing and then mitigating an incident.

Ms. GIBSON. So much of this has been done at the local level in the past, and that will continue. And you get into a terrorist attack, you have all these other issues coming in, law enforcement will be there, it's just a different scenario.

I think DHS, their role is at the prevention of all this to try to assess the threats and figure out how to prevent them from hap-

pening. And then as far as consequences I don't think there's a whole lot of change from how it would have been anyway.

Mr. SHAYS. See, what I suspect is—and we've been along this, but what I suspect is that there is a part of the chemical industry that doesn't want people to be alarmed by the various scenarios because some of the scenarios are quite frightening and so it doesn't want to push that.

What I am fearing is that we aren't leveling with ourselves as to what the consequence could be and so—and because we're not doing that, we're leaving our constituency very vulnerable. That's what I feel.

Mr. DURBIN. But I think you raise that and that's a separate issue. I would agree with you there's a lot of improvement that has to take place in the way of information sharing, even at the level of DHS trying to tell just the private sector and the different critical infrastructure sectors about what we should be prepared for.

I mean, this is an evolving role here that we don't have it perfect yet, and DHS gets certain intelligence information and they're running through their own processes figuring out how much they can tell us, how much they can't, protecting sources and methods. And then they find themselves getting into a situation where they say, well, now we've cleansed so much information out of it, if we do provide it to anybody it's not of any use.

So, I mean, there's no question there's real challenges as far as providing the right types of information out both to the public and to the sectors themselves.

Mr. STEPHENSON. You know, there's not a standard model here. When you look at the other 13 infrastructure elements DHS does not have the lead for all 13 of those. EPA still has the water and—

Mr. SHAYS. Slow down. They don't have the role for what.

Mr. STEPHENSON. DHS does not have the lead role, the lead Federal agency role for all 13 infrastructure elements. There's not a single model that applies. For example, EPA is still the lead for the water infrastructure, Agriculture is still the lead for food security and the likes. If you look at all those 13 infrastructure elements that are set out in the administration's Homeland Security Plan, DHS doesn't control them all.

So there are different models that work in different infrastructure segments. So, who the lead agency should be is maybe not a simple answer, maybe it's one that needs to be studied.

Mr. SHAYS. And there are 13 infrastructure areas.

Mr. STEPHENSON. There are, yeah, 13 stated in the President's Homeland Security Strategy.

Mr. SHAYS. Thank you, Mr. Chairman.

Mr. STEPHENSON. For example, power companies are a key.

Mr. SHAYS. Let me ask you, is there anything that the four of you would like to respond to based on any question of the first panel, just any information you need to correct or get out on the table or you need to just agree with or disagree with.

Mr. STEPHENSON. The main thing I would reiterate is need for Federal legislation requiring vulnerability assessments of the chemical sector. There is a Federal requirement for most sectors,

but at this point such a requirement is curiously absent from this sector.

Mr. SHAYS. And there is that consensus, then, agreed, which is helpful. Thank you.

Mr. STEPHENSON. That's our point of view.

Mr. MURPHY. Anybody else who wishes to add any comments for the panel?

Ms. WITMER. Just one thing, and it's sort of a minor point. I don't remember which of you had asked whether or not there were emergency evacuation plans in place, and, in fact, there are as part of the risk management plans that companies have had to develop. And those, as you had mentioned, regardless of whether it's an accidental release or a terrorism-related incident, that emergency management plan would kick in and, you know, people would be evacuated.

Mr. SHAYS. See, the difference is before—can I go, Mr. Chairman?

Mr. MURPHY. [Nods affirmatively.]

Mr. SHAYS. We did a review of Y-12 and their evacuation plan and this is a nuclear—is it a processing site.

Mr. HALLORAN. Manufacturing.

Mr. SHAYS. Pardon me.

Mr. HALLORAN. Manufacturing.

Mr. SHAYS. Manufacturing.

But what was interesting is when they thought of it only in terms of safety—when they thought of it in terms of terrorism, those willing to go up in flames with it, it always was you had to come in and you had to get out, and so the scenario was such that they didn't need as many people because even if someone got inside, they still had to get out and so they wouldn't be able to take the material and get away.

Well, you know, now with terrorism they don't have to come in and take away, they just have to come in, and they could come in under sight; in other words, the assumption has totally changed and we realized all these sites were vulnerable around the country.

In other words, someone willing to be a suicide bomber becomes a whole different scenario. And so what I wonder about these plans is if you have a circumstance now where you are basically saying that you could have someone on the inside, you could have three vats instead of one, you could have someone blow up a road. Then your scenario is totally different, and I'm not struck by the fact that we're even coming close to dealing with evacuation plans based on that.

I realize that, you know, we would want to put focus on the plants that are most likely to be attacked, I mean, there's some in the countryside, there's some—and I realize we're going to be getting half of what we need to get done today to start paperwork and things like that. I just wonder who's dealing with it, and I don't feel anyone is really right now.

Mr. MURPHY. I'd like to thank all the witnesses from both panels today for being here. You've helped us a great deal and we will attempt to report an understanding of the Federal Government's role in this.

I would think that if there's any fear I have of what comes out of these—well, two fears. One is overreaction and one is underreaction. Looking around the room I can't put my eyes on anything in this room that did not have some level of manufacturing impact by the chemical industry, everything that is involved in our lives, and we are dependent upon it. This is not an attack of the chemical industry, this is what we know and are responsible with the chemical industries to be involved with changes.

My fear of other reaction is, and particularly in an election year, that there will be so much politicization of these issues that some people will say the threat is exaggerated.

I pulled up an article from the Internet regarding risk of chemical plants. This was published in 2000, and basically it was pooh-poohing the whole idea that there have been terrorist attacks on this country and we didn't have to worry about that. What a naive concept that was and I think we're still involved with that.

I appreciate your candor and we don't have any further questions for this panel, but we have to get answers to these issues and continue to protect the American public.

Mr. SHAYS. And if I could also thank you for hosting this hearing. It was important, I think, for us to be out in the field, and I do appreciate our panel very much. Thank you.

Mr. MURPHY. Thank you, Mr. Shays, Mr. Turner, for coming out here to visit us.

Mr. SHAYS. And, Transcriber, you did it with a smile the whole time.

Mr. MURPHY. This hearing is adjourned.

NOTE.—The General Accounting Office report entitled, "Homeland Security, Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown," may be found in subcommittee files.]

[Whereupon, at 1 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

GREGORI LEBEDEV
PRESIDENT AND
CHIEF EXECUTIVE OFFICER



February 26, 2004

The Honorable David M. Walker
Comptroller General
General Accounting Office
441 G Street, NW, Room 7100
Washington, DC 20548

Re: GAO's Testimony on February 23 Regarding
Chemical Facility Security

Dear Mr. Walker:

The American Chemistry Council was pleased that GAO's John Stephenson and our Security Team leader Marty Durbin were able to testify together Monday at a field hearing of a House subcommittee on the subject of chemical facility security. We appreciated Mr. Stephenson's oral statement, which complimented the substantial accomplishments of our association's members, and we continue to concur with GAO's recommendation that Congress enact comprehensive legislation in this area. However, we do have some concerns with the written testimony GAO released that day¹ – which has received broad press coverage – and wanted to make sure you had the benefit of our comments on it.

ACC represents the leading companies engaged in the business of chemistry, and our members are responsible for about 90% of basic chemical production in the United States. The business of chemistry is a \$460 billion enterprise and a critical element of the nation's economic infrastructure. It is the nation's largest exporter,

¹ U.S. General Accounting Office, *Homeland Security: Federal Action Needed to Address Security Challenges at Chemical Facilities*, GAO-04-482T (Washington, D.C.: Feb. 23, 2004).



Responsible Care®

1300 Wilson Boulevard, Arlington, VA 22209 • Telephone 703-741-5100 • Fax 703-741-6086

The Honorable David M. Walker
February 26, 2004
Page 2

accounting for more than ten cents out of every dollar in U.S. exports. Our members represent more than half a million employees, at nearly 1700 facilities throughout the United States. The business of chemistry is the original knowledge industry investing more in research and development than any other business sector, and accounting for 1 in 8 patents issued in this country.

Safety and security have always been primary concerns of ACC members, and since 9/11 they have only intensified their efforts, working closely with government at all levels, to improve security and to defend against any threat to the nation's critical infrastructure.

GAO's testimony was drawn almost entirely from its excellent March 2003 report on chemical facility security.² Thus, the testimony detailed the aggressive steps our membership has taken, "[t]o its credit," to reduce security risks, focusing on our Responsible Care Security Code. It also described ACC members' "commendable" partnerships with governmental agencies at all levels, including our operation with the Department of Homeland Security of an Information Sharing & Analysis Center to collect and share threat data. The report also noted our work to drive these actions beyond our association's membership. Finally, it repeated GAO's call, which ACC has long endorsed, for federal legislation that would require all chemical facilities to assess their vulnerabilities and implement security measures.

GAO's March 2003 report was generally accurate at the time it was released. However, much has changed since then to improve our nation's security. Unfortunately, these changes have rendered portions of the report, and some testimony drawn from it, out-of-date in describing both our members' implementation of the Security Code and the federal government's efforts over the past year. Also, in condensing the report to summary form, the testimony made several statements that were incorrect or misleading.

² U.S. General Accounting Office. *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-459 (Washington, D.C.: Mar. 14, 2003).

The Honorable David M. Walker
February 26, 2004
Page 3

As to ACC members' accomplishments:

1. The testimony says "ACC reports that the 120 facilities ranked as the highest risk and 372 facilities ranked as the next highest have completed vulnerability assessments."³ That was the case last summer. Since then, all ACC member facilities (including another 1460 plants) have completed these assessments. Top tier facilities were required to complete implementation of their security enhancements by the end of last year, and those enhancements will be verified by outside third parties by March 31st.

2. The testimony at one point accurately states that ACC's Security Code third party verification process does not address whether a "facility has conducted the vulnerability assessment appropriately or that its actions adequately address security risks."⁴ In other places, however, the GAO's testimony states simply: "ACC does not verify implementation . . . of security measures"⁵ or "no . . . third-party verification ensures that security vulnerabilities are addressed."⁶ In fact, the Security Code's third party verification *does* involve determining whether physical security measures chosen to reduce vulnerabilities were implemented. To go further – making judgments about the appropriateness of a vulnerability assessment or the adequacy of particular measures is very difficult without access to accurate and complete threat information. As the testimony notes, the private sector needs better threat information.

As to the federal government's accomplishments:

1. The testimony states that "chemical facilities are not subject to any federal requirements to assess and address security vulnerabilities against terrorist attacks."⁷ Actually, under the Maritime Transportation Security Act (MTSA), some 4,000 facilities, including most of the largest chemical plants, are explicitly

³ Testimony at 12.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.* at "What GAO Found" and p. 3.

⁷ *Id.* at 3.

The Honorable David M. Walker
February 26, 2004
Page 4

required to do this, subject to stringent Coast Guard oversight. The testimony several times notes that the MTSA requires "some" chemical facilities "to develop security plans,"⁸ but there is much more to the MTSA than that. Most important, the Coast Guard is reviewing the submissions of every facility required to do an assessment and plan under that law and is empowered to require more if need be. Furthermore, it will begin inspecting facilities for compliance in July.

2. The statement that "neither EPA nor DHS is currently monitoring the extent to which the industry has implemented security measures,"⁹ while true last March, is not correct now. In the past year, DHS's Information Analysis and Infrastructure Protection (IAIP) Directorate has been visiting chemical facilities, assessing their vulnerabilities, evaluating their security measures and coordinating with state and local law enforcement and emergency responders with responsibility for these facilities. Further, we concur with the President's designation of DHS – a security-focused agency – rather than EPA as the lead agency to oversee security for this critical sector.

3. Similarly, it is no longer accurate to say that, "[d]espite a congressional mandate to do so, the federal government has not conducted the assessments necessary to develop comprehensive information on the chemical industry's vulnerabilities to terrorist attacks."¹⁰ IAIP has been engaged in precisely this effort for the last year and has already issued several documents on the topic, although not publicly.

As you can see, both our members and the federal government have made great strides separately and together in the past year to enhance the security of the chemical sector. And ACC continues to agree with GAO that comprehensive federal security legislation should be enacted to empower DHS to require all facilities to address security vulnerabilities. We will aggressively continue our efforts to make such legislation a reality, and GAO's important work in this area is

⁸ *Id.* at 6, 8.

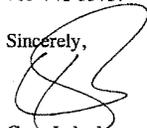
⁹ *Id.* at "What GAO Found" and p. 11.

¹⁰ *Id.* at 10.

The Honorable David M. Walker
February 26, 2004
Page 5

a tool to help accomplish that important objective. We, of course, remain ready to assist GAO in this area and others; and please feel free to contact Marty Durbin at 703-741-5575.

Sincerely,



Greg Lebedev
President and
Chief Executive Officer

cc: John B. Stephenson